# OX230 / OX250 / OX350I

# WiMAX Outdoor CPE

# User Manual

**Version: 1.0**

**Date: Jan. 12, 2011**

# Table of Contents

1. Introduction ..... 10
1.1. Connect ..... 10
1.2. Logout ..... 11
2. Status ..... 12
2.1. WiMAX Status ..... 12
2.2. Network Status ..... 12
2.3. Device Status ..... 13
3. Personalization ..... 14
3.1. Account ..... 14
3.2. Date ..... 15
3.2.1. Date ..... 15
3.2.2. Time Zone ..... 16
4. WiMAX ..... 17
4.1. Scanner ..... 17
4.2. Authentication ..... 19
4.3. Wide Scan ..... 22
5. Networking ..... 24
5.1. Bridge/NAT mode ..... 24
5.1.1. LAN ..... 24
5.1.2. WAN ..... 24

5.1.3. DNS....26
5.2. Firewall....27
5.2.1. HTTP....28
5.2.2. TELNET....28
5.2.3. DMZ....28
5.2.4. IP Filiter....29
5.3. DHCP Server....31
5.4. NAT ALG....34
5.5. Forwarding....35
5.6. Trigger....36
5.7. DDNS....37
5.8. UPnP....38
5.8.1. UPnP Setting....38
5.9. Ping....39
6. Management....40
6.1. TR-069....40
6.2. OMA-DM....41
6.3. SNMP....43
6.4. Log....43
6.5. Upgrade....44
6.6. Recovery....45
7. VPN....46

7.1. PPTP.....46

7.1.1. PPTP Server .....46

7.1.2. PPTP Client.....48

7.2. L2TP .....50

7.2.1. L2TP Server .....50

7.2.2. L2TP Client.....53

7.3. IPsec.....54

# List of Figures

Figure 1 Login ..... 11

Figure 2 Logout ..... 11

Figure 3 Status>WiMAX Status ..... 12

Figure 4 Status>Network Status ..... 13

Figure 5 Status>Device Status ..... 13

Figure 6 Personalization>Account ..... 14

Figure 7 Personalization>Date>Date ..... 15

Figure 8 Personalization>Date>Time Zone ..... 16

Figure 9 Wireless Broadband Access ..... 17

Figure 10 WiMAX>Scanner ..... 18

Figure 11 WiMAX>Authentication(No authentication) ..... 19

Figure 12 WiMAX>Authentication(User authentication) ..... 20

Figure 13 WiMAX>Wide Scan ..... 22

Figure 14 Networking>Bridge/NAT mode>LAN ..... 24

Figure 15 Networking>Bridge/NAT mode>WAN ..... 25

Figure 16 Networking>Bridge/NAT mode>DNS ..... 27

Figure 17 Networking>Firewall>HTTP ..... 28

Figure 18 Networking>Firewall>TELNET ..... 28

Figure 19 Networking>Firewall>DMZ ..... 29

Figure 20 Networking>Firewall>IP Filter ..... 29

Figure 21 Networking>DHCP Server ..... 32
Figure 22 Networking>NAT ALG ..... 34
Figure 23 Networking>Forwarding ..... 35
Figure 24 Networking>Trigger ..... 36
Figure 25 Networking>DDNS ..... 37
Figure 26 Networking>UPnP ..... 38
Figure 27 Networking>Ping ..... 39
Figure 28 Management>TR-069 ..... 40
Figure 29 Management>OMA-DM ..... 42
Figure 30 Management>SNMP ..... 43
Figure 31 Management>Log ..... 44
Figure 32 Management>Upgrade ..... 44
Figure 33 Management>Recovery ..... 45
Figure 34 Restore to factory reset warning ..... 45
Figure 35 VPN>PPTP>PPTP Server ..... 47
Figure 36 VPN>PPTP>PPTP Client ..... 49
Figure 37 VPN>PPTP>PPTP Client>Add ..... 49
Figure 38 VPN>L2TP>L2TP Server ..... 51
Figure 39 VPN>L2TP>L2TP Client ..... 53
Figure 40 VPN>L2TP>L2TP Client>Add ..... 53
Figure 41 VPN>IPsec Overview ..... 54
Figure 42 VPN>IPsec>Add ..... 55

# List of Tables

Table 1 Field definition for Personalization>Account ..... 15

Table 2 Field definition for Personalization>Date>Date ..... 16

Table 3 Field definition for Personalization>Date>Time Zone ..... 16

Table 4 Field definition for WiMAX>Scanner ..... 19

Table 5 Field definition for WiMAX>Authentication ..... 22

Table 6 Field definition for WiMAX>Wide Scan ..... 23

Table 7 Field definition for Networking>Bridge/NAT mode>LAN ..... 24

Table 8 Field definition for Networking>Bridge/NAT mode>WAN ..... 26

Table 9 Field definition for Networking>Bridge/NAT mode>DNS ..... 27

Table 10 Field definition for Networking>Firewall>HTTP ..... 28

Table 11 Field definition for Networking>Firewall>TELNET ..... 28

Table 12 Field definition for Networking>Firewall>IP Filter ..... 30

Table 13 Field definition for Networking>DHCP Server ..... 34

Table 14 Field definition for Networking>Forwarding ..... 36

Table 15 Field definition for Networking>Trigger ..... 37

Table 16 Field definition for Networking>DDNS ..... 38

Table 17 Field definition for Networking>UPnP ..... 39

Table 18 Field definition for Networking>Ping ..... 39

Table 19 Field definition for Management>TR-069 ..... 41

Table 20 Field definition for Management>OMA-DM ..... 42

Table 21 Field definition for Management>SNMP ..... 43

Table 22 Field definition for Management>Upgrade ..... 45

Table 23 Field definition for VPN>PPTP>PPTP Server ..... 48

Table 24 Field definition for VPN>PPTP>PPTP Client ..... 50

Table 25 Field definition for VPN>L2TP>L2TP Server ..... 52

Table 26 Field definition for VPN>L2TP>L2TP Client ..... 54

Table 27 Field definition for VPN>IPsec>Add ..... 59

# 1. Introduction

The CPE Software platform comes with a Web-based Configuration Manager, which gives users the ability to manage, configure and analyze the platforms environment. The Connection Manager works with all versions of Windows after Windows 95.

**The supported browser version:**

- Internet Explorer Ver 8.0 or later (Recommended)
- FireFox Ver.3.6 and higher
- Google Chrome Ver.5.0 and higher

## 1.1. Connect

Users need to connect to the CPE platform. It's assumed that the user has a fully working CPE platform and properly connected. From the web browser connect to the device, entering the IP address of the device; it will prompt user to enter the username and password, as shown in Figure 1. The default IP address, usernames and passwords are as follows.

**Default IP Address**

- 192.168.0.254

**Username/Password**

- admin/admin
- guest/guest

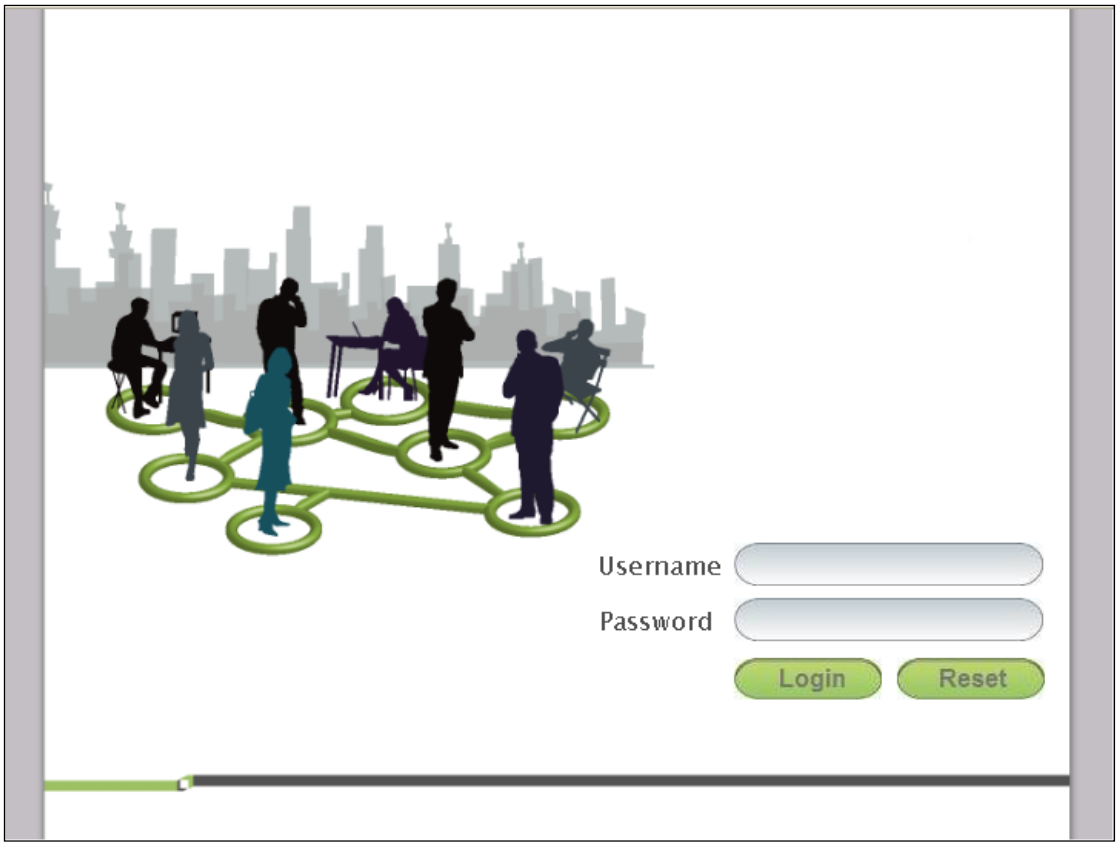


Figure 1 Login

# 1.2. Logout

The “Logout” window allows users to disconnect from the device and exit the Web-based Configuration Manager as shown in Figure 2.

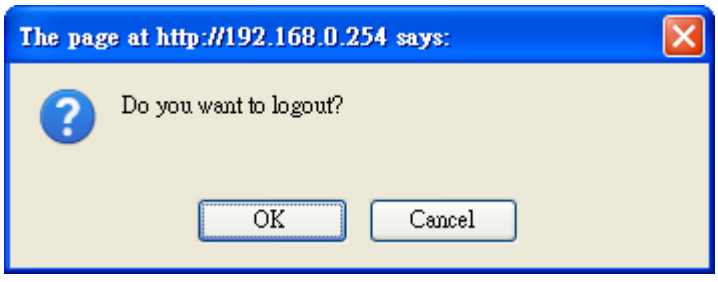


Figure 2 Logout

# 2. Status

After user has established a connection, user will see the “Status” window. It gives user an initial overview of the current status of the device.

## 2.1. WiMAX Status

This window shows the information of system status, WiMAX link status and service flow status.

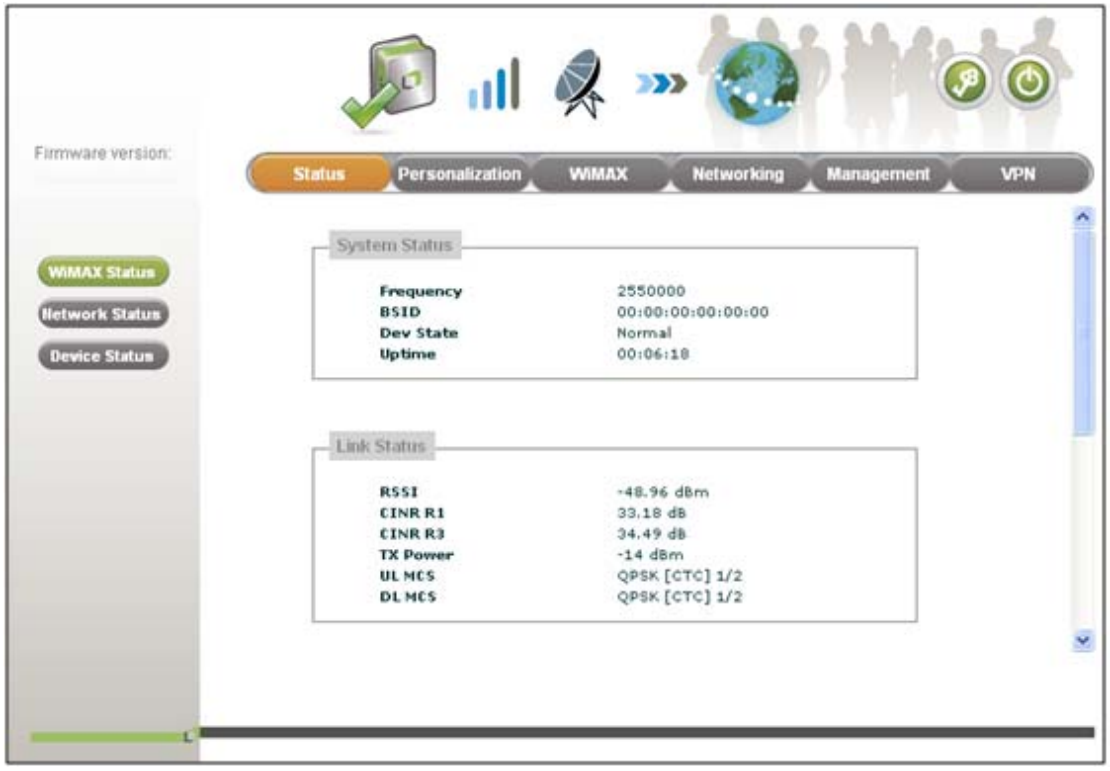


Figure 3 Status>WiMAX Status

## 2.2. Network Status

The “Network Status” displays the information of WAN status and LAN status as shown in Figure 4.

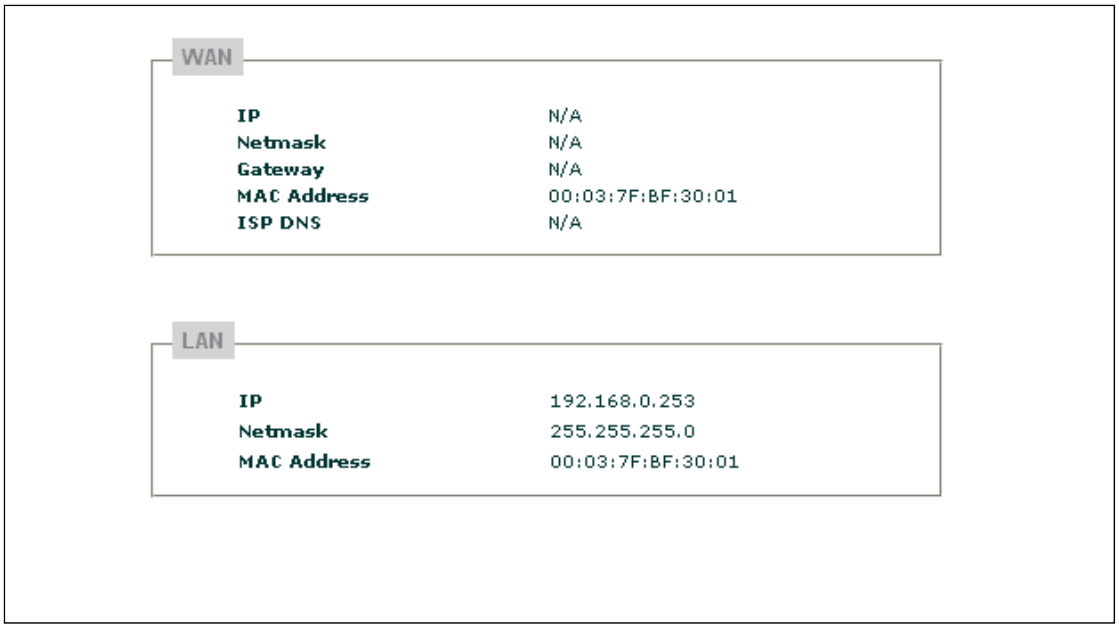


Figure 4 Status>Network Status

# 2.3. Device Status

The “Device Status” displays the information of device status as shown in Figure 5.

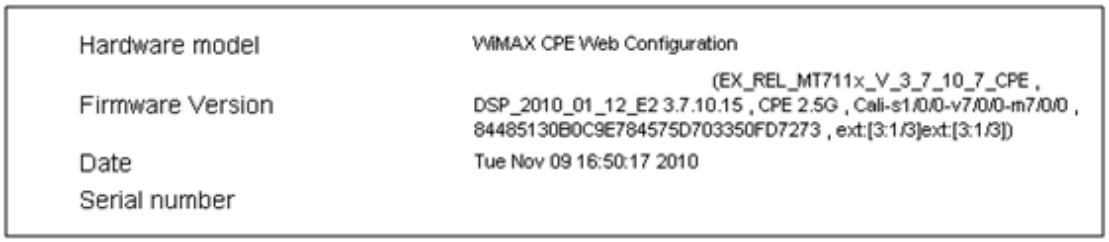
Hardware model
WiMAX CPE Web Configuration
Firmware Version
(EX_REL_MT711x_V_3_7_10_7_CPE , DSP_2010_01_12_E2 3.7.10.15 , CPE 2.5G , Cali-s1/0/0-v7/0/0-m7/0/0 , 84485130B0C9E784575D703350FD7273 , ext:[3:1/3]ext:[3:1/3])
Date
Tue Nov 09 16:50:17 2010
Serial number

Figure 5 Status>Device Status

# 3. Personalization

## 3.1. Account

Note: The default usernames/passwords are admin/admin and guest/guest.

The user with administrative privileges (belonging to the “admin” group) has access to all the features in the software. A user with “guest” privileges (belonging to the “guest” group) only has a subset of the features available to them.

Note: There can only be one username in each of the groups (one to one relationship).

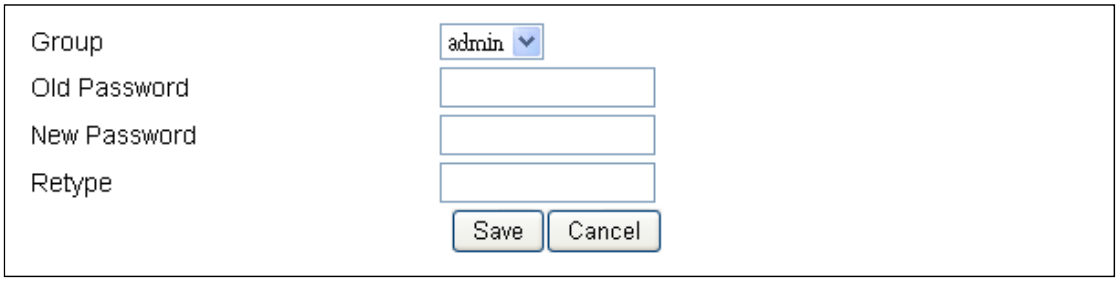


Figure 6 Personalization>Account

| Name | Description |
|---|---|
| **Change Password** | |
| Group | Select which group the user belongs to that user would like to change the password for.<br><br>admin, if the user is part of the admin group, they have full access to all the features.<br><br>guest, if the user is part of the guest group, they have limited access to the features. |
| Old Password | Enter the old password. |
| New Password | Enter the new password. |
| Retype | Retype the new password. |
| Save | Commit the changes made and save to CPE, it will only commit the change made to the password. |
| Cancel | Reset fields to the last saved values. |

Table 1 Field definition for Personalization>Account

# 3.2. Date

## 3.2.1. Date

User can configure date and time on the device as shown in Figure 7. Each field definition is shown on Table 2. User can manually configure the system time, or choose to get the date and time from a time server. The “Save” button will commit the configuration, and the “Cancel” button will clear the fields.

Note: If user doesn’t configure the time on the CPE it will use the default system starting time. The default system starting time is set to 1970/1/1 00:00:00

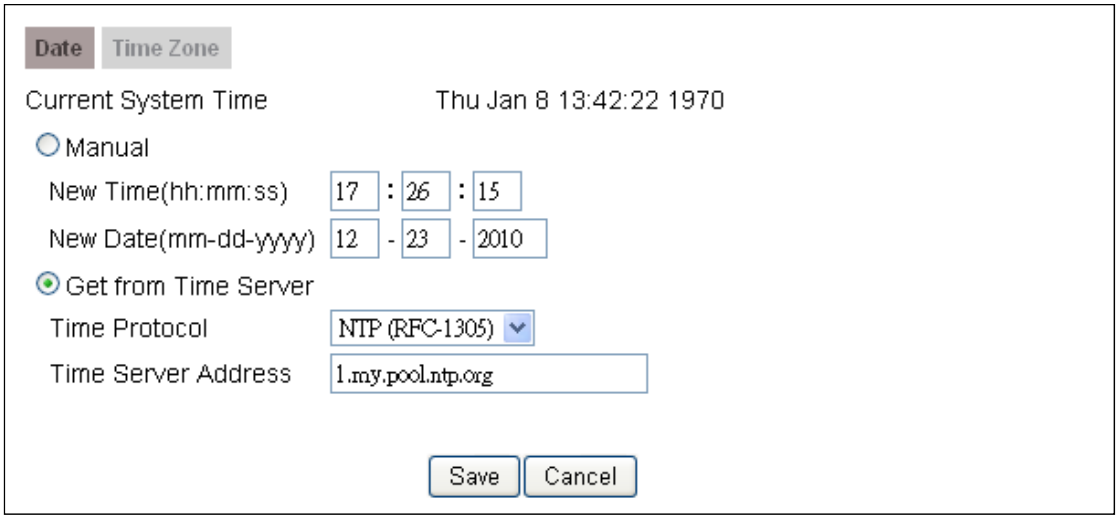


Figure 7 Personalization>Date>Date

| Name | Description |
|---|---|
| Manual | If user selects the Manual option, then user needs to enter the time and date manually. |
| New Time | New time manually entered |
| New Date | New date manually entered |
| Get From Time Server | If user selects this option it will get the local time from a time server automatically. |
| Time Protocol | Select the Time protocol |
| Time Server Address | Enter the address of the time server. |
| Save | Commit the changes made and save to CPE |

| Name | Description |
|---|---|
| Cancel | Reset fields to the last saved values |

Table 2 Field definition for Personalization>Date>Date

## 3.2.2. Time Zone

The “Time Zone” tab will allow user to set the time zone and set the starting and finish time for daylight saving period as shown in Figure 8. The definition for each field is shown on Table 3. User can also enable or disable “Daylight Savings Time”.

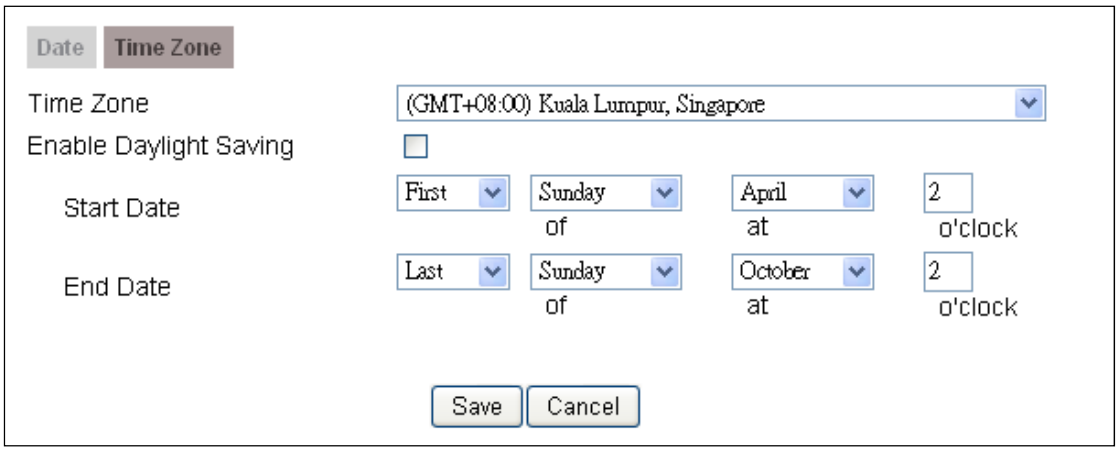


Figure 8 Personalization>Date>Time Zone

| Name | Description |
|---|---|
| Time Zone | Enter the time zone of for the location |
| Enable Daylight Savings | If user wants to enable Daylight Savings Time, user needs to check the box. |
| Start Date | Enter the beginning date for Daylight Savings time |
| End Date | Enter the end date for Daylight Savings time. |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 3 Field definition for Personalization>Date>Time Zone

# 4. WiMAX

This technology is based on the IEEE 802.16 standard, enabling the delivery of last mile wireless broadband access.

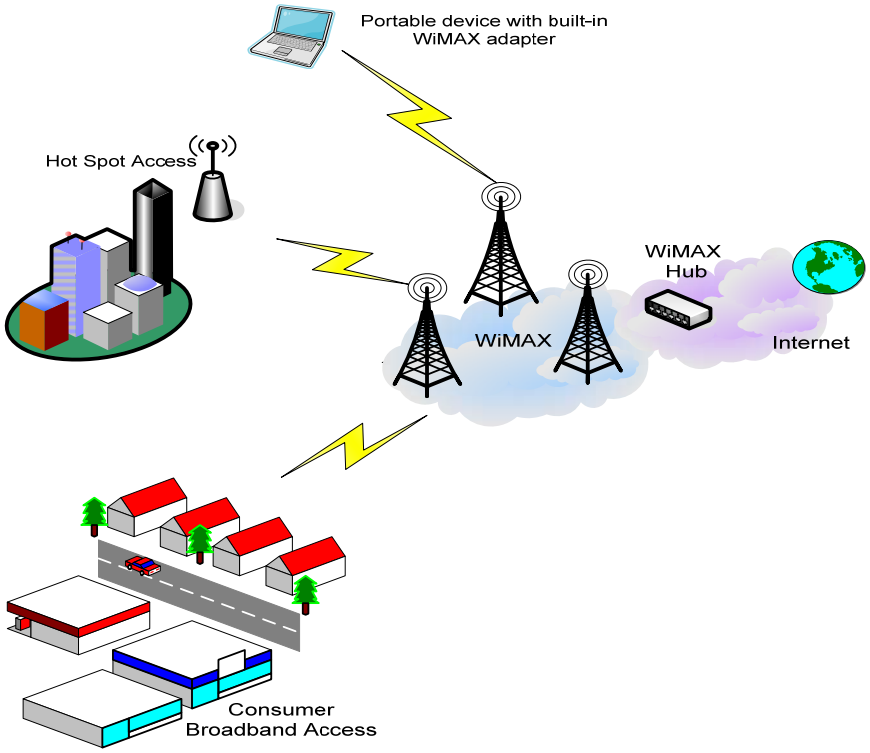


Figure 9 Wireless Broadband Access

## 4.1. Scanner

User can set WiMAX standard settings, which include how to establish a connection and get frequency information as shown in Figure 10. The definition for each field is shown on Table 4.

The frequency list window displays all the configured frequencies and their bandwidth. To set additional frequencies, click on the “Add” button.

Figure 10 WiMAX>Scanner

| Name | Description |
|---|---|
| Start | Click the “Start” button to connect to a BSID |
| Stop | Click the “Stop” button to terminate the connection |
| Search | Click the “Search” button to scan the frequency |
| Joint Wide Scan Result | Yes means to append wide scan result to the frequency setting. |
| Default Bandwidth | Select the default bandwidth to be used in Frequency List<br>● 5 MHz<br>● 7 MHz<br>● 10 MHz |

| Name | Description |
|---|---|
| Valid Band Info | Valid band information. If the frequencies aren't located using the valid band range, the frequency setting will be rejected. |
| Add | The "Add" button will allow user to enter more frequency lists |
| OK | Click the "OK" button to exit table edit mode |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 4 Field definition for WiMAX>Scanner

# 4.2. Authentication

Figure 11 WiMAX>Authentication(No authentication)

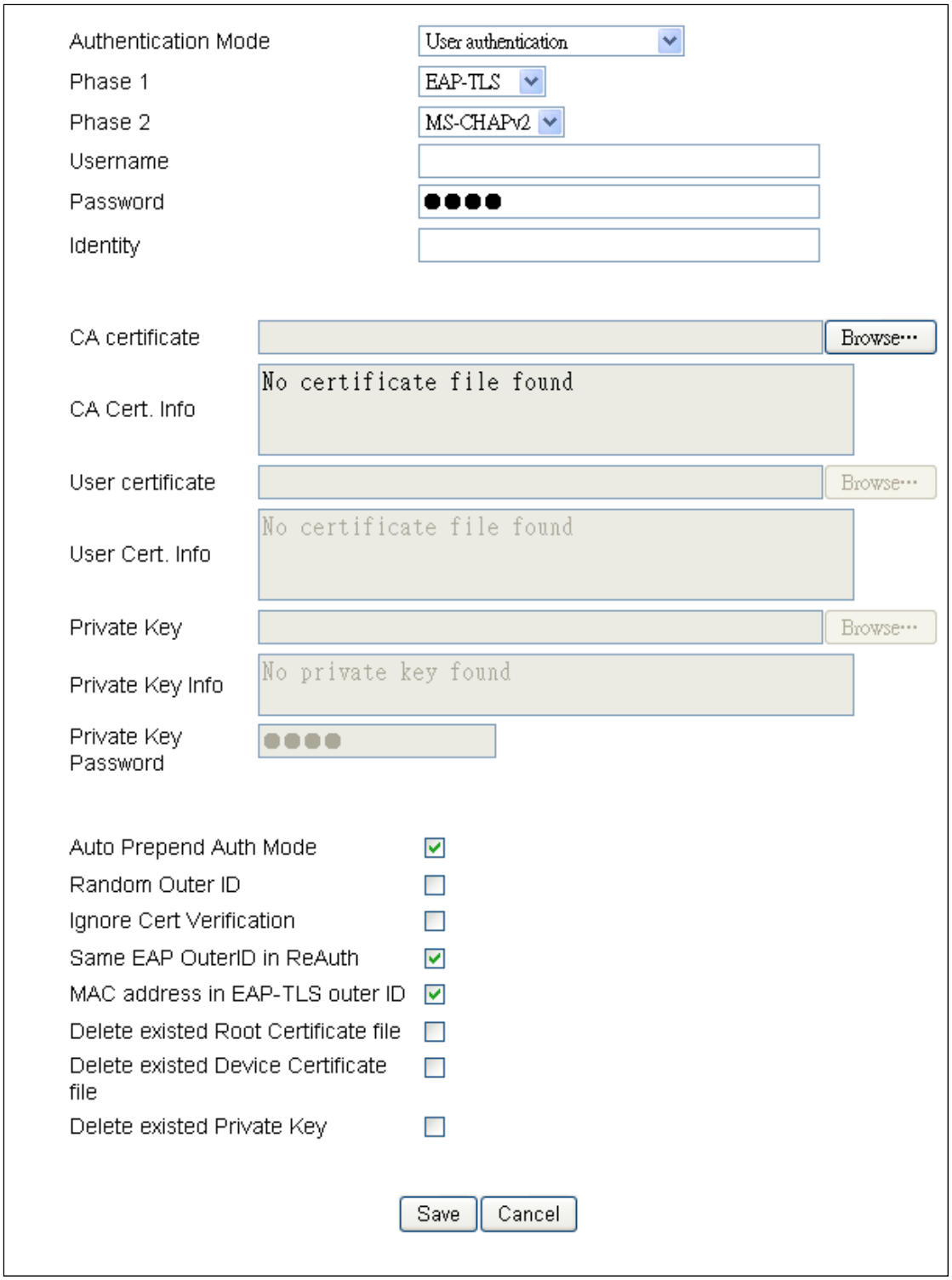


Figure 12 WiMAX>Authentication(User authentication)

| Name | Description |
|---|---|
| **Authentication** | |
| Authentication Mode | The method used in authentication.<br>● No Authentication<br>● User Authentication |

| Name | Description |
|---|---|
| | ● Device Authentication<br>● User and Device Authentication |
| **EAP Supplicant** | |
| Phase 1 | The EAP method used in authentication |
| Phase 2 | The inner method |
| User name | The user name used in inner method |
| Password | The password used in inner method. |
| Identity | The identity encoded in EAP Identity Response message. User needs to fill the Outer ID at this field. |
| CA certificate | The root CA's X.509 certificate. |
| CA Cert. Info | The root CA's certificate information. |
| User certificate | The MS's X.509 certificate. |
| User Cert. Info | The root MS's certificate information. |
| Private Key | The MS's private key file corresponding to the public key enhanced in x.509 certificate |
| Private Key Info | The MS's private key information. |
| Private Key Password | The key used to decrypt the MS's private key file |
| **Options** | |
| Auto Prepend Auth Mode | puts {am=i} in EAP outer ID<br>i = 1: user authentication<br>i = 2: device authentication<br>i = 3: user & device authentication |
| Random Outer ID | Enable MS to generate 16-bytes random number as the user name in the EAP Identity Response message. |
| Ignore Cert Verification | MS skips to verify the BS's certificate received in the EAP-TLS or EAP-TTLS procedure. |
| Same EAP Outer ID in ReAuth | Use the same EAP outer ID when doing re-auth |
| MAC address in EAP-TLS outer ID | Add MAC address in outer ID when EAP mode is EAP-TLS |
| Delete existed Root Certificate file | Remove the files loaded from UI |
| Delete existed Device Certificate file | Delete device certificate file which was uploaded in the field "MTK-authorized Device Certificate" |
| Delete existed Pri- | Delete device private key which was uploaded in the |

| Name | Description |
|---|---|
| vate Key | field “Device Private Key” |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 5 Field definition for WiMAX>Authentication

# 4.3. Wide Scan

The “Wide Scan” function is used for scanning BS based on scanning rule. User can set the scan rule with defining start, stop frequency, step, and channel bandwidth, and CPE will base on this rule to scan the BS as shown in Figure 13. The definition for each field is shown on Table 6.

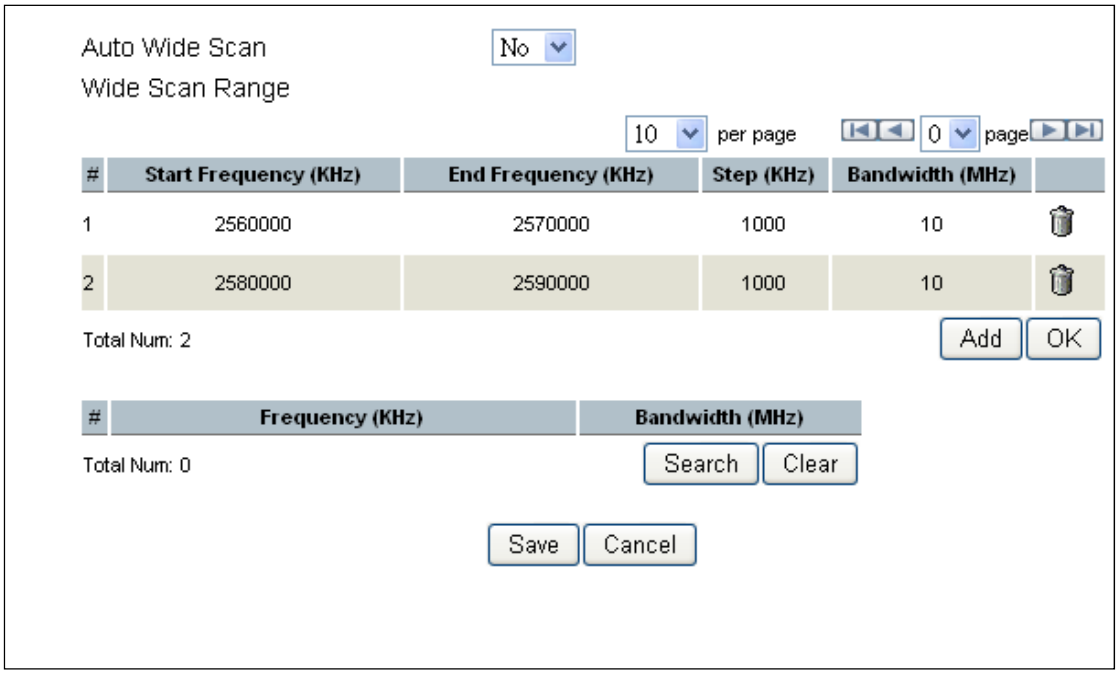


Figure 13 WiMAX>Wide Scan

| Name | Description |
|---|---|
| Auto Wide Scan | Select “Yes” to do “wide scan” automatically when there are no available BS |
| **Wide Scan Range** | |
| Add/OK | User can specify the wide scan range to reduce search time |
| **Wide Scan Result** | |
| Search | Show the result of wide scan. Search button can trigger |

| Name | Description |
|---|---|
| | wide scan |
| Clear | Clear button clear current search result |
| Save/Cancel | Save/Cancel current setting |

Table 6 Field definition for WiMAX>Wide Scan

# 5. Networking

## 5.1. Bridge/NAT mode

### 5.1.1. LAN

From the “Networking>Bridge/NAT mode>LAN” window, user can update the LAN information as shown in Figure 14. The definition for each field is shown on Table 7.

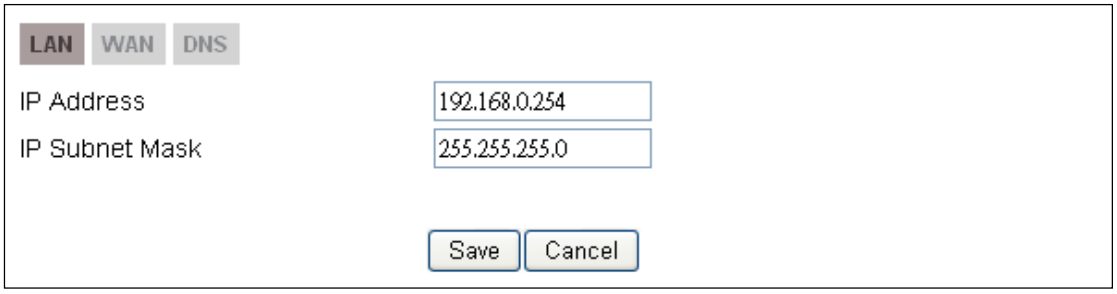


Figure 14 Networking>Bridge/NAT mode>LAN

| Name | Description |
|---|---|
| IP Address | IP address of CPE |
| IP Subnet Mask | Subnet Mask of CPE |
| Save | Commits the changes made, and set the LAN IP information, some services will be reloaded. |
| Cancel | Reset the fields to the last saved values |

Table 7 Field definition for Networking>Bridge/NAT mode>LAN

### 5.1.2. WAN

In Figure 15, it demonstrates how to configure WAN IP on CPE web page. In this web page, the PPPoE setting will be shown if user choose “PPPoE” for “WAN Protocol”. The definition for each field is shown on Table 8.

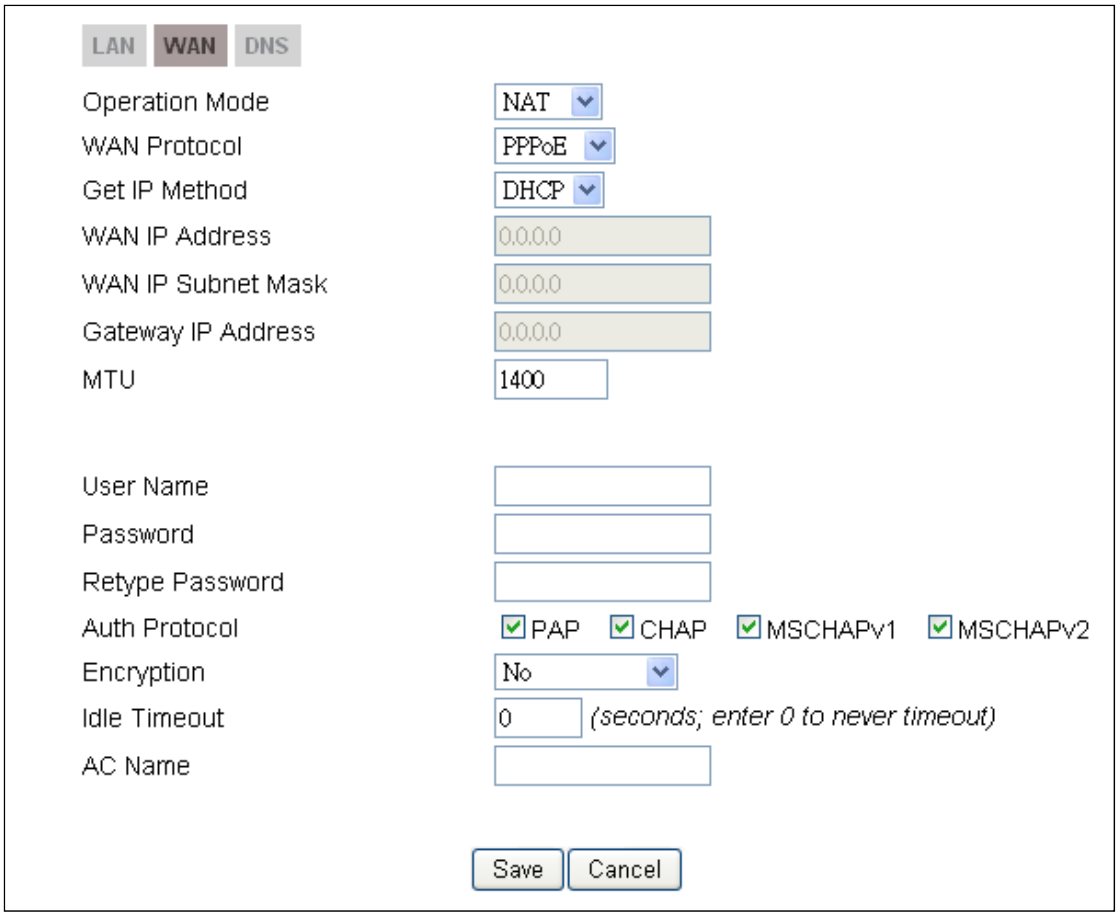


Figure 15 Networking>Bridge/NAT mode>WAN

| Name | Description |
|---|---|
| **WAN IP** | |
| Operation Mode | Select the WAN operation mode<br>● Bridge<br>● NAT |
| WAN Protocol | Select the WAN encapsulation protocol<br>● Ethernet<br>● PPPoE |
| Get IP Method | Select the IP method<br>● DHCP<br>● Static |
| WAN IP Address | If user chooses “Static” for IP Method, user should enter the WAN IP address |
| WIN IP Subnet Mask | If user chooses “Static” for IP Method, user should enter the WAN IP subnet mask. |
| Gateway IP Address | If user chooses “Static” for IP Method, user should enter IP gateway address |

| Name | Description |
|---|---|
| MTU | Enter the MTU |
| **PPPoE** | |
| User Name | The user name to connect PPPoE server via the selected Auth Protocol |
| Password | The password of the corresponding username |
| Retype Password | Type the “Password” again |
| Auth Protocol | The authentication protocol of the peer required. Select which Authentication protocol to use.<br>● PAP<br>● CHAP<br>● MSCHAPv1<br>● MSCHAPv2 |
| Encryption | Encryption Scheme<br>● No<br>● MPPE 40 bits: 40-bit encryption with MPPE<br>● MPPE 128 bits: 128-bit encryption with MPPE<br>● Auto: automatically selected |
| Idle Timeout | Disconnect if the link is idle for the assigned seconds |
| AC Name | The name of the access concentrator to connection to |
| Save | Commit the changes made and save to CPE, after clicking the Save button user will get a message asking if user wants to reboot the CPE. Reboot is necessary for the device to switch to a different profile. |
| Cancel | Reset field to the last saved values |

Table 8 Field definition for Networking>Bridge/NAT mode>WAN

## 5.1.3. DNS

In Figure 16, it demonstrates how to configure WAN DNS on CPE web page. The definition for each field is shown on Table 9.

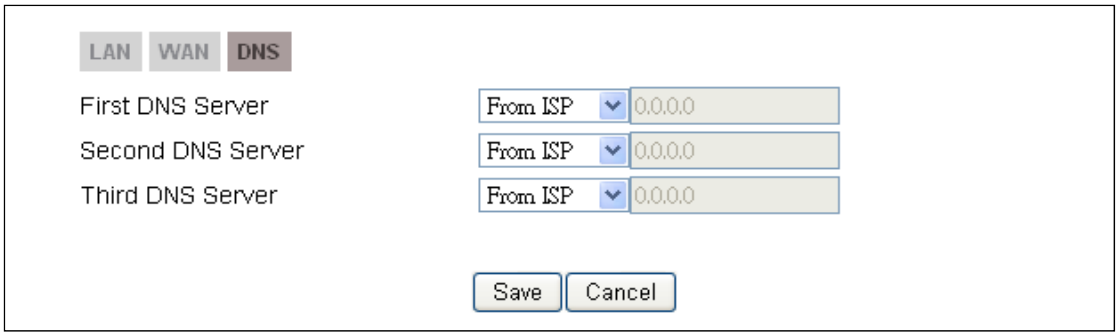


Figure 16 Networking>Bridge/NAT mode>DNS

| Name | Description |
|---|---|
| First DNS Server | Enter the WAN DNS information.<br>● User Defined<br>● From ISP<br><br>If user selects “User Define”, user needs to enter a valid IP address for the DNS server. |
| Second DNS Server | Same as First DNS Server |
| Third DNS Server | Same as First DNS Server |
| Save | Commit the changes made and save to CPE, after clicking the Save button user will get a message asking if user wants to reboot the CPE. Reboot is necessary for the device to switch to a different profile. |
| Cancel | Reset field to the last saved values |

Table 9 Field definition for Networking>Bridge/NAT mode>DNS

# 5.2. Firewall

In networking, firewalls are used to block un-wanted traffic. It will prevent unauthorized devices to enter a trusted network.

## 5.2.1. HTTP

Figure 17 Networking>Firewall>HTTP

| Name | Description |
|---|---|
| Allow Web accessing from WAN | Check the check-box to allow connections from WAN. |
| Save | Commit the changes made and save to CPE. |
| Cancel | Reset fields to the last saved values. |

Table 10 Field definition for Networking>Firewall>HTTP

## 5.2.2. TELNET

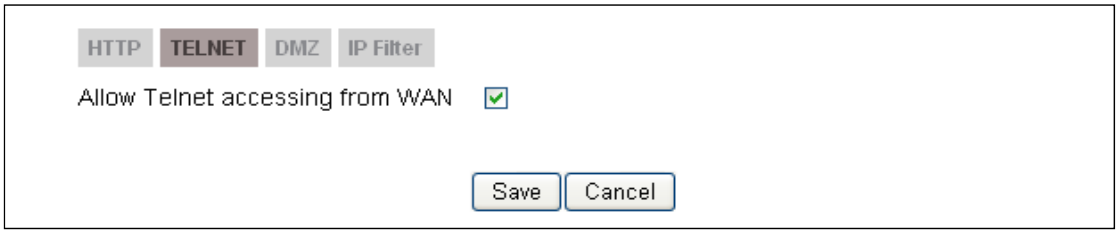


Figure 18 Networking>Firewall>TELNET

| Name | Description |
|---|---|
| Allow Telnet access-ing from WAN | Check the check-box to allow connections from WAN. |
| Save | Commit the changes made and save to CPE. |
| Cancel | Reset fields to the last saved values. |

Table 11 Field definition for Networking>Firewall>TELNET

## 5.2.3. DMZ

DMZ stands for Demilitarized Zone. It is a physical or logical sub-network that

contains and exposes an organization's external services to a larger un-trusted network, usually the Internet. The term is normally referred to as a DMZ by IT professionals. It is sometimes referred to as a Perimeter Network. The purpose of a DMZ is to add an additional layer of security to an organization's LAN; an external attacker only has access to equipment in the DMZ, rather than any other part of the network.

The “Networking>Firewall>DMZ” tab allows user to configure a DMZ host IP address as shown in Figure 19. In DMZ Settings, user needs to enter the IP address of the DMZ host. The “Save” button will save the changes to CPE and the “Cancel” button will reset the field to last saved value. It will disable DMZ host when entering “0.0.0.0”.

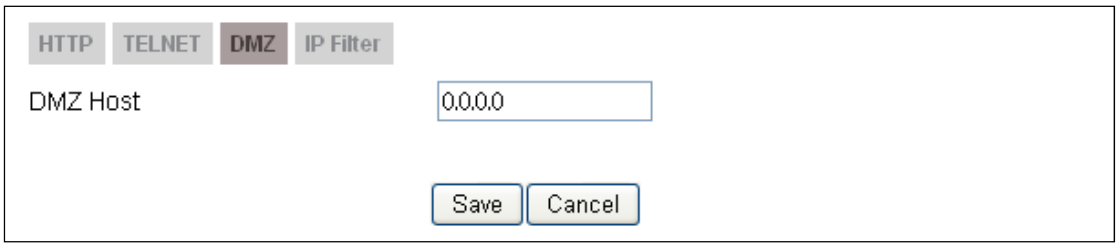


Figure 19 Networking>Firewall>DMZ

## 5.2.4. IP Filiter

The IP filter rules will drop or discard traffic that fits the filter criteria. User can define IP filter rules as shown in Figure 20. The definition for each field is shown on Table 12.

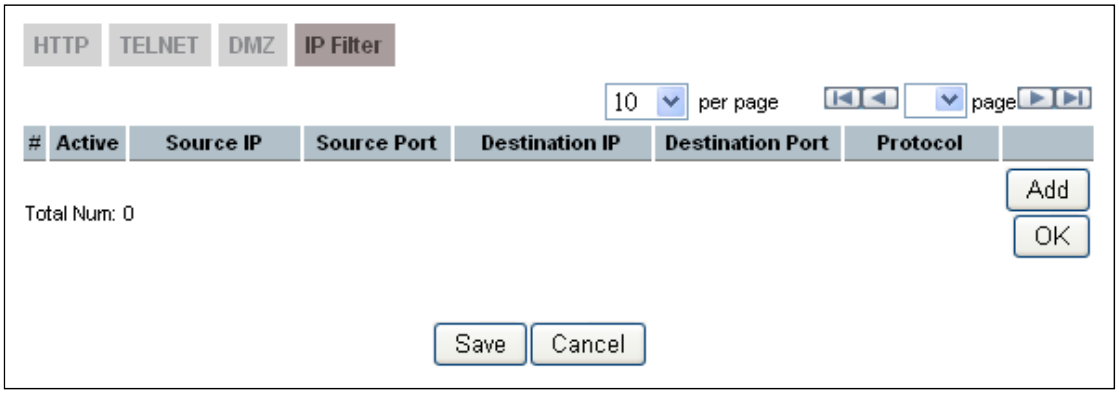


Figure 20 Networking>Firewall>IP Filter

| Name | Description |
|---|---|

| Name | Description |
|---|---|
| Add | Click the "Add" button to create a new IP Filter rule |
| OK | Click the "OK" button will exit the table edit mode |
| Active | Check the box to activate the IP Filter rule |
| Source IP | Source IP to filter on. It can be in one of the following formats:<br>IP address (ex. 192.168.0.222)<br>Subnet (ex. 192.168.1.0/24)<br>IP range (ex. 192.168.0.150~192.168.0.160)<br>0.0.0.0/0 means any |
| Source Port | Source Port to filter on. It can be one of the following formats:<br>Port number (ex. 8080)<br>Port Range (ex. 1024~2048) |
| Destination IP | Destination IP to filter on. It can be in one of the following formats:<br>IP address (ex. 192.168.0.222)<br>Subnet (ex. 192.168.1.0/24)<br>IP range (ex. 192.168.0.150~192.168.0.160)<br>0.0.0.0/0 means any |
| Destination Port | Destination port to filter on. It can be one of the following formats:<br>Port number (ex. 8080)<br>Port Range (ex. 1024~2048) |
| Protocol | Protocol to filter on |
| Trash | Delete the IP Filter rule |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 12 Field definition for Networking>Firewall>IP Filter

# 5.3. DHCP Server

Use the “Networking> DHCP Server” tab to configure the DHCP server information. The default DHCP Server setup is enabled, and user could disable this function from setup as shown in Figure 21. When user disables the DHCP server, it requires setting a static IP address on host PC for CPE to configure. Please be noted that without the static IP address set properly on the host PC, user can not open the CPE web page for configuration.

When DHCP server is enabled, user needs to define the IP pool range for dynamically assigning the IP address. The advantage of using DHCP server is that the addresses which are no longer in use will be returned to the IP address pool so that the server can reallocate them to other machines in the network. There are three DNS servers the user can configure to assign an IP address. Static DHCP will assign an IP address on the LAN to a specific device based on its MAC address. The definition for each field is shown on Table 13.

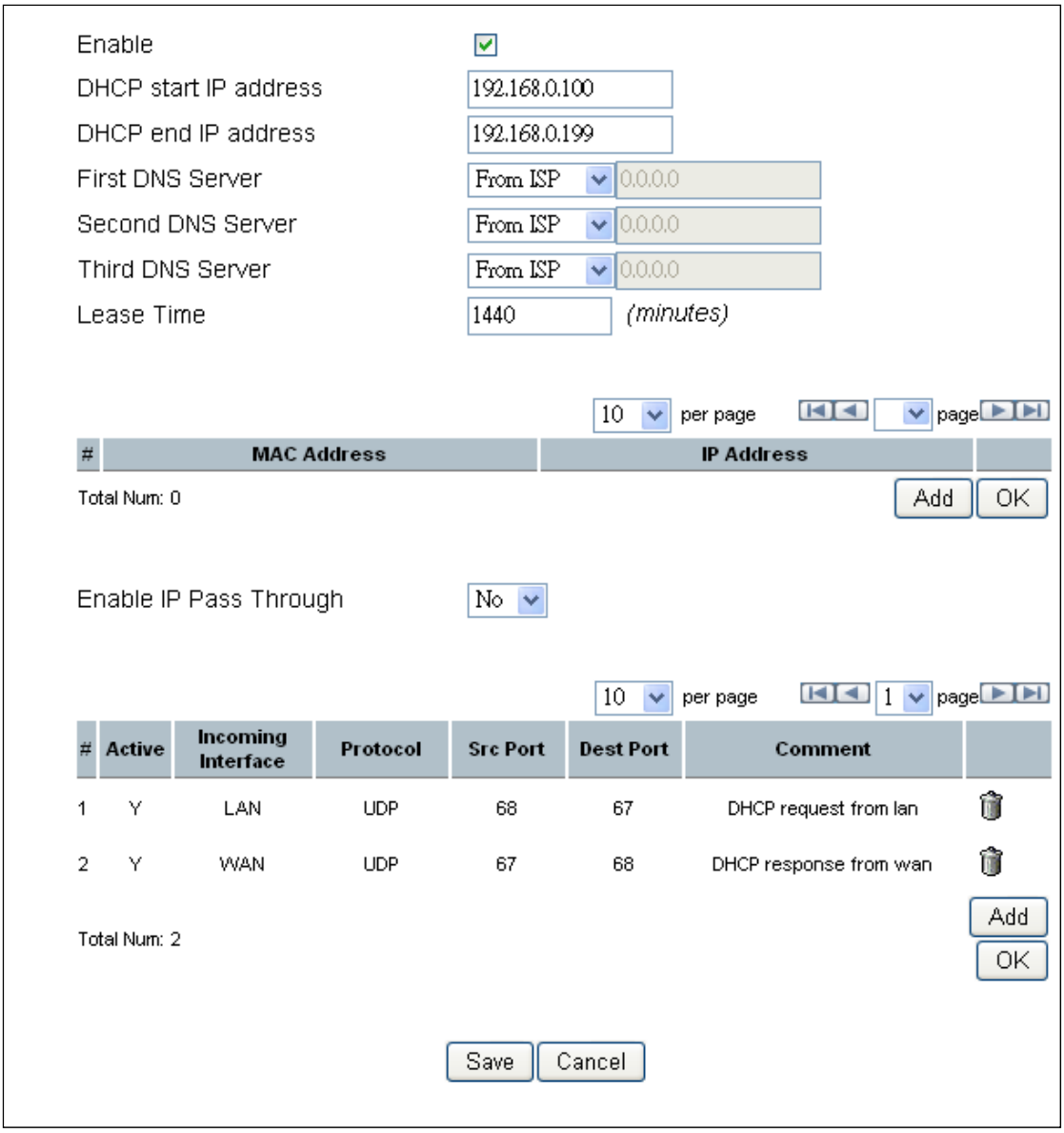


Figure 21 Networking>DHCP Server

| Name | Description |
|---|---|
| Enable | Check the check-box to enable DHCP server. |
| DHCP start IP address | Starting IP address range |
| DHCP end IP address | Ending IP address range |
| Lease Time | The lease time is a controlled time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed (dynamic re-use of IP addresses). Lease time is measured in minutes in the Configuration Manager. |

| Name | Description |
|---|---|
| First DNS Server<br><br>Second DNS Server<br><br>Third DNS Server | User can specify three DNS servers and select how the DNS Server is assigned. There are three options for assigning the DNS server.<br>● From ISP<br>● User Defined<br>● None<br><br>If user selects “None”, then the DHCP server will not give clients the DNS server information. If all the three DNS servers setting are set to “None”, then the DHCP server will use the LAN IP address as the DNS server information for the clients. If the user chooses “User Defined” and leaves the IP address as “0.0.0.0” it will change the field to “None”. |
| Static DHCP | Enter MAC address and IP address for static DHCP addresses. |
| Add | Click on the “Add” button to enter a static leased IP address. Enter the MAC address of the Ethernet device and enter the IP address. |
| OK | Click the “OK” button to exit out of edit mode. |
| Enable IP Pass Through | Yes means to enable IP pass through function. |
| Active | Check the check-box to activate the IP pass through rule |
| Incoming Interface | There are three options for assigning the incoming interface.<br>● ALL<br>● LAN<br>● WAN |
| Protocol | There are three options for assigning the protocol.<br>● TCP/UDP<br>● UDP<br>● TCP |
| Src Port | Source port for packet incoming. The format of this field is as below:<br><br>Port number (ex. 8080) |

| Name | Description |
|---|---|
| Dest Port | Destination port for packet outgoing. The format of this field is as below:<br><br>Port number (ex. 8080) |
| Comment | Description of the rule |
| Trash | Delete the IP Pass Through rule |
| Save | Commit the changes made and save to CPE, some services will be reloaded. |
| Cancel | Reset fields to the last saved values. |

Table 13 Field definition for Networking>DHCP Server

# 5.4. NAT ALG

There are some ALG settings that user can enable from “Networking>NAT ALG”. ALG allows legitimate application traffic to pass through the CPE that would have otherwise restricted. Without ALGs, some application may not work well because of NAT/firewall settings. User could click on the check box to enable ALGs.

Note: If user is using any of these types of application protocols user needs to enable them in the ALG settings.

- FTP ALG
- H.323 ALG
- PPTP ALG
- SIP ALG Set BSID

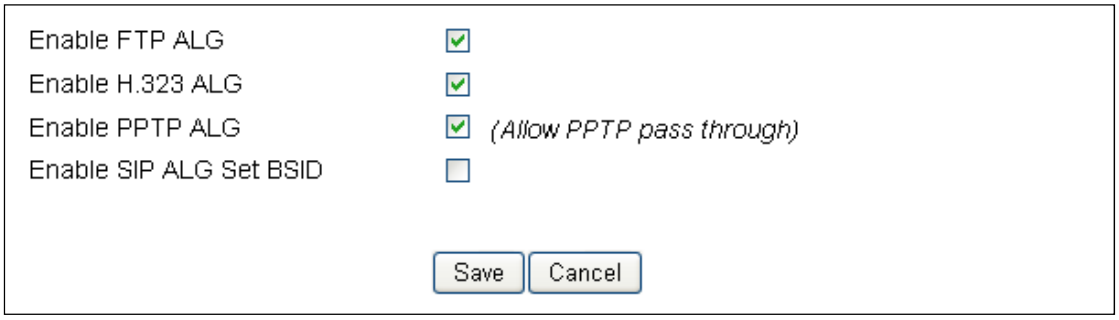


Figure 22 Networking>NAT ALG

# 5.5. Forwarding

Forwarding is the act of forwarding the data from WAN side to the particular port of the private IP. This function can allow remote computers to reach a port on a private IP address within a private LAN. In the following, it will introduce how to setup for Port Forward. First, user needs to click the “Add” button and then select which forward type, TCP or UDP or TCP/UDP, is preferred to trigger the special application as shown in Figure 23. User needs to assign some specific port for the WAN IP to be forwarded to the defined LAN IP and port, and then click the “Save” button to add a Port Forward rule. The definition for each field is shown on Table 14.

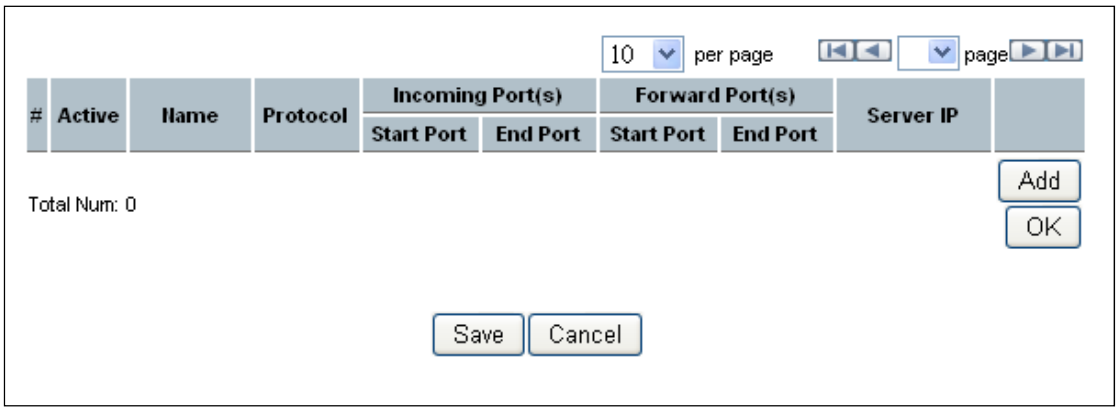


Figure 23 Networking>Forwarding

| Name | Description |
|---|---|
| Active | Check the box to active the port forward rule |
| Name | Name of the port forward rule |
| Protocol | User needs to define the desired protocol for rule. Available options are: TCP, UDP, or TCP/UDP |
| Incoming Port(s) | User needs to define incoming port range for port forwarding rule. |
| Forward Port(s) | User needs to define to which port range will be translated for port forwarding rule. The packet will be forwarded to one of these ports if it matches the rule. |
| Server IP | User needs to define which IP address will be translated to if it matches the Port Forwarding rule. The packet will be forwarded to this IP address if it matches the rule. |
| Trash | Delete the Port Forward rule |

| Name | Description |
|---|---|
| Add | Click the “Add” button to create a new Port Forward rule |
| OK | Click the “OK” button to exit table edit mode |
| Save | Commit the changes made and save to the CPE |
| Cancel | Reset field to the last saved values. |

Table 14 Field definition for Networking>Forwarding

# 5.6. Trigger

The “Networking>Trigger” allows user to configure Port Trigger rules as shown in Figure 24. Port Trigger is a way to automate port forwarding in which outbound traffic on predetermined ports (‘trigger port’) causes inbound traffic to specific incoming ports to be dynamically forwarded to the initiating host, while the outbound ports are in use. This allows users behind CPE on the LAN to provide services that would normally require the computer to have IP address on the LAN. Port triggering triggers an open incoming port (‘open port’) when a client on the local network makes an outgoing connection on a predetermined port or range of ports. The definition for each field is shown on Table 15.

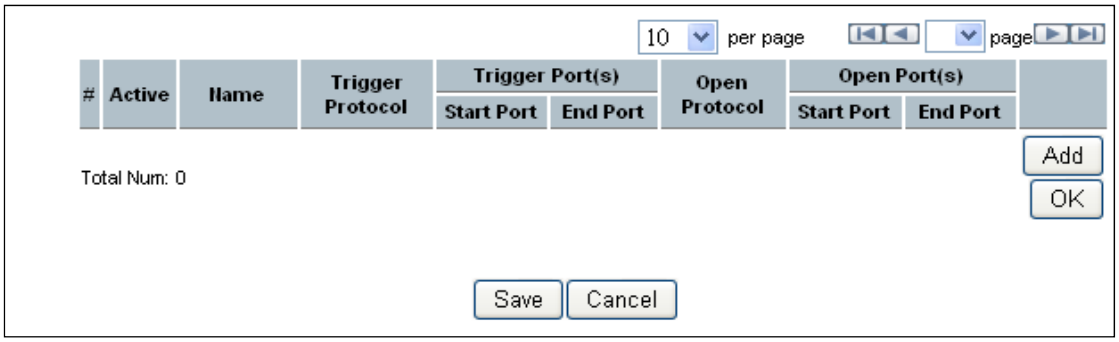


Figure 24 Networking>Trigger

| Name | Description |
|---|---|
| Active | Check the box to active the Port Trigger rule |
| Name | Name of the Port Trigger rule |
| Trigger Protocol | It defines which protocol the outgoing packet used will trigger the rule. Available options are TCP, UDP or TCP/UDP |
| Trigger Port(s) | It defines which port range the outgoing packet will trigger the rule. User needs to enter the starting and |

| Name | Description |
|---|---|
| | ending port range |
| Open Protocol | It defines which protocol will be opened if the rule had been triggered. Available options are TCP, UDP or TCP/UDP |
| Open Port(s) | It defines which protocol port will be opened if the rule had been triggered. User needs to enter the starting and ending port range |
| Trash | Delete the Port Trigger rule |
| Add | Click the “Add” button to enter a Port Trigger rule |
| OK | Click the “OK” button to exit, table edit mode. |
| Save | Commit the changes made and save to the CPE |
| Cancel | Reset fields to the last saved values |

Table 15 Field definition for Networking>Trigger

# 5.7. DDNS

DDNS stands for Dynamic Domain Name Services. It provides a function to convert the domain name to the unique IP address. With DDNS, users is able to find and connect to CPE no matter what IP address CPE is currently using, that is, DDNS can map CPE's dynamic IP address to a static hostname. The best profit of this function allows user to access CPE from everywhere.

In Figure 25, it demonstrates how to configure DDNS on CPE web page. The definition for each field is shown on Table 16.

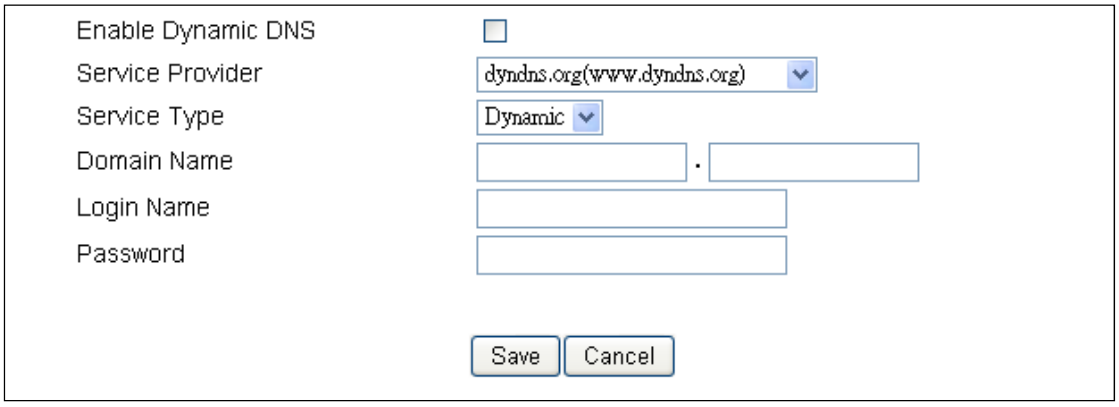


Figure 25 Networking>DDNS

| Name | Description |
|---|---|

| Name | Description |
|---|---|
| Enable Dynamic DNS | Click the checkbox to enable dynamic DNS |
| Service Provider | Enter the URL of the Service Provider |
| Service Type* | Enter the service type (DYNDNS only)<br>● Dynamic<br>● Static<br>● Custom |
| Domain Name | Enter the domain name |
| Login Name | Enter the username |
| Password | Enter the password |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Note: * Supported by DYNDNS service provider.

Table 16 Field definition for Networking>DDNS

# 5.8. UPnP

Two methods of simplifying the process of connecting a device to the network are available as shown in Figure 26. UPnP allows devices to connect seamlessly to networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components. NAT Port Mapping Protocol (NAP-PMP) allows a computer in a private network (behind a NAT router) to automatically configure the router to allow parties outside the private network to contact itself. The definition for each field of UPnP Setting is shown on Table 17.

## 5.8.1. UPnP Setting

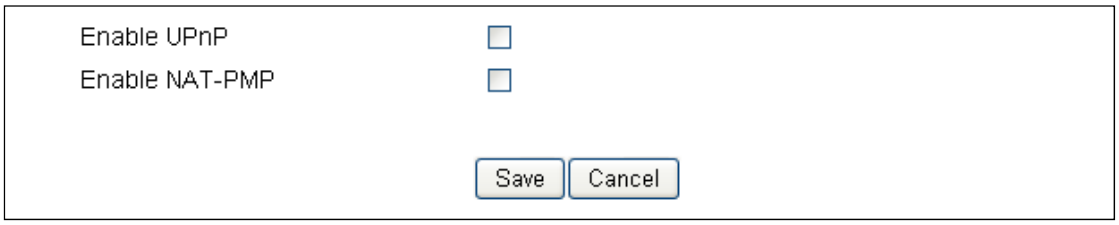


Figure 26 Networking>UPnP

| Name | Description |
|---|---|

| Name | Description |
|---|---|
| Enable UPnP | Check the check box to enable UPnP |
| Enable NAT-PMP | Check the check box to enable NAT-PMP |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 17 Field definition for Networking>UPnP

# 5.9. Ping

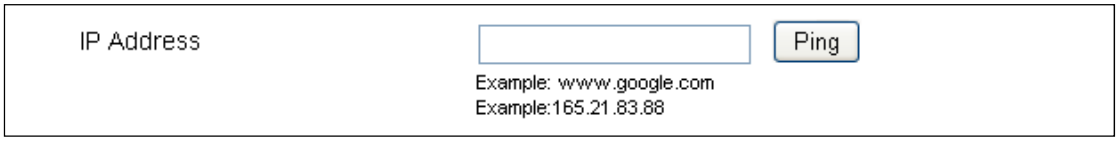


Figure 27 Networking>Ping

| Name | Description |
|---|---|
| IP Address | The destination IP address for ping test. It can be in one of the following formats:<br>● IP address (ex. 165.21.83.88)<br>● Domain name (ex. www.google.com) |
| Ping | Commit the ping test request |

Table 18 Field definition for Networking>Ping

# 6. Management

## 6.1. TR-069

Using TR-069 the terminals can communicate with the Auto Configuration Servers (ACS) and establish the configuration automatically as shown in Figure 28. The definition for each field of TR-069 is shown on Table 19. It's the current standard for activation of terminals in the DSL broadband market.

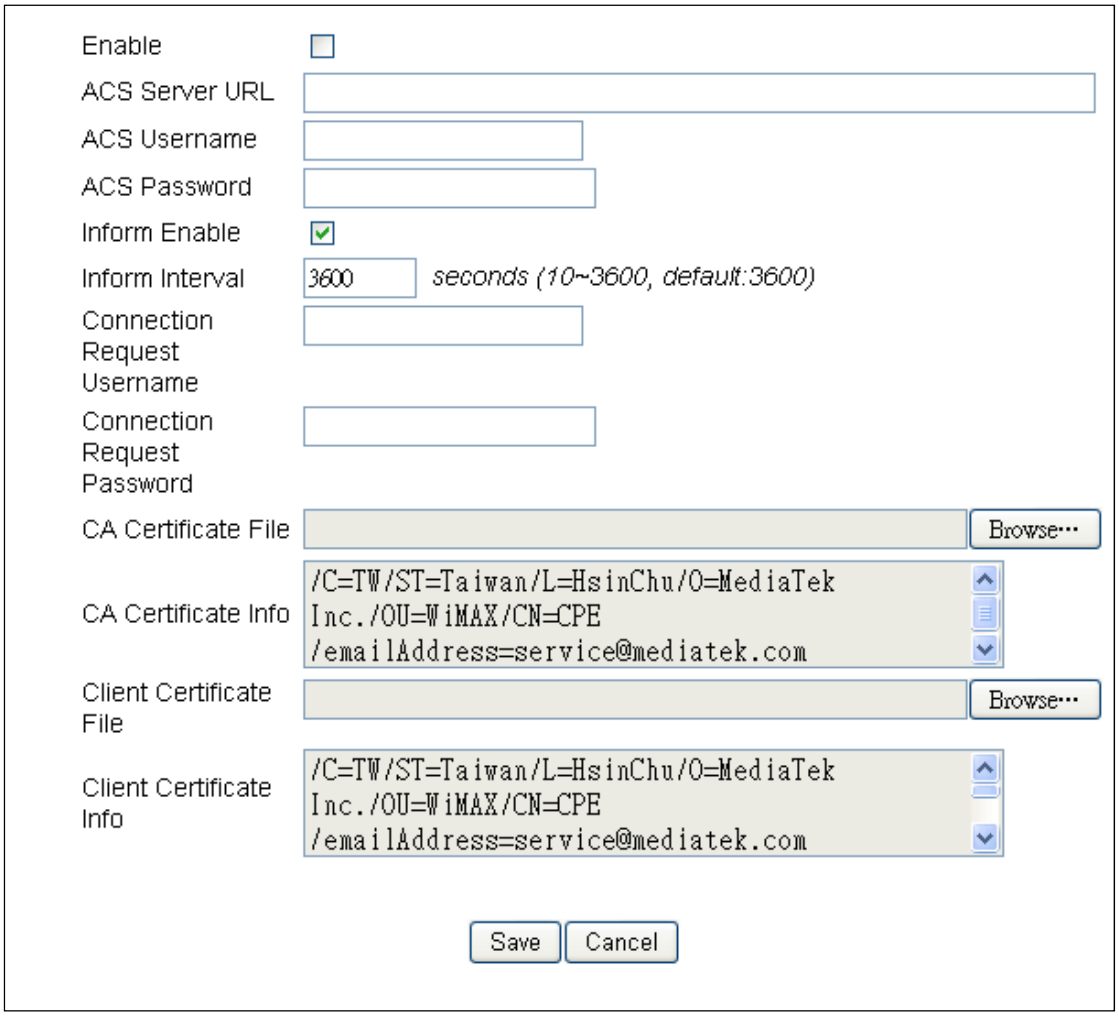


Figure 28 Management>TR-069

| Name | Description |
|---|---|
| Enable | To enable or disable the TR-069 activity on the CPE. |
| Fixed Client Port | To specify fixed client port |
| ACS Server URL | The ACS URL for CPE to connect to. |

| Name | Description |
|---|---|
| Bootstrap Enable | Check the box to enable bootstrap. |
| ACS Username | The username for the CPE when connected to ACS. |
| ACS Password | The password for the CPE when connected to ACS. |
| Periodical Inform Enable | To enable or disable the periodical inform to ACS for CPE. |
| Periodical Inform Interval | The interval between two periodical inform. |
| Connection Request Username | Enter the username for the ACS to perform connection request to CPE. |
| Connection Request Password | Enter the password for the ACS to perform connection request to CPE. |
| CA Certificate File | The CA certificate file is used to identify the certificate of ACS when D-230 communicated ACS with HTTPS URL. |
| CA Certificate Info | Displays the subject field of the CA Certificate. |
| Client Certificate File | The CLIENT certificate file is used when CPE communicates with HTTPS URL. |
| Client Certificate Info | Displays the subject field of the CLIENT Certificate. |
| Save | Commit the changes made and save to CPE. |
| Cancel | Reset fields to the last saved values. |

Table 19 Field definition for Management>TR-069

# 6.2. OMA-DM

Using OMA DM the terminals can communicate with the OMA DM Server and establish the configuration automatically as shown in Figure 29. The definition for each field of OMA-DM is shown on Table 20. It’s the current standard for activation of terminals in OMA (Open Mobile Alliance).

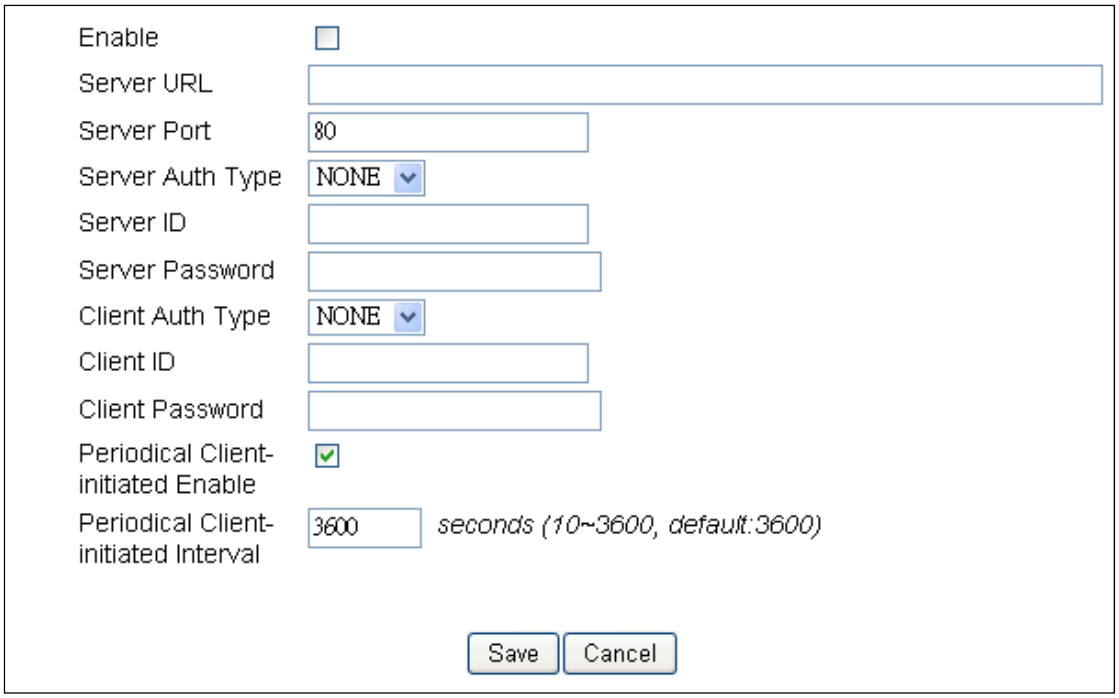


Figure 29 Management>OMA-DM

| Name | Description |
|---|---|
| Enable | To enable or disable the OMA-DM activity of CPE. |
| Server URL | The DM Server URL for CPE to connect to. |
| Server Port | The DM Server Port for CPE to connect to. |
| Server Auth Type | The DM Server authentication type. |
| Server ID | The Server ID for CPE when connected to DM Server. |
| Server Password | The Server password for CPE when connected to DM Server. |
| Client Auth Type | The DM Client authentication type. |
| Client ID | The Client ID for CPE when connected to DM Server. |
| Client Password | The Client password for CPE when connected to DM Server. |
| Periodical Client-initiated Enable | To enable or disable the periodical client-initiated session to DM server for CPE. |
| Periodical Client-initiated Interval | The interval between two periodical client-initiated sessions. |
| Save | Commit the changes made and save to CPE. |
| Cancel | Reset fields to the last saved values. |

Table 20 Field definition for Management>OMA-DM

# 6.3. SNMP

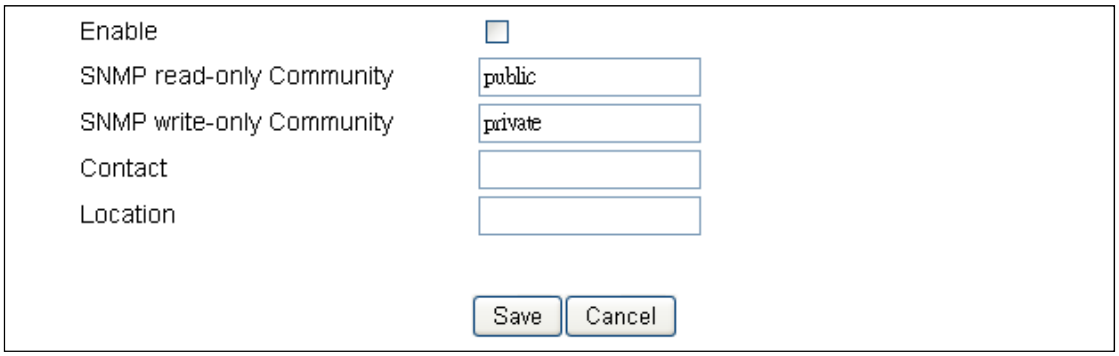


Figure 30 Management>SNMP

| Name | Description |
|---|---|
| Enable | Checking the enable button will allow SNMP applications to query and set some of the SNMP variables. |
| Location | Enter the Location SNMP string variable. |
| Contact | Enter the Contact SNMP string variable. |
| SNMP read-only Community | Enter Read community string to query SNMP data. |
| SNMP write-only Community | Enter Write community string to query SNMP variables. |
| Save | Commit the changes made and save to CPE. |
| Cancel | Reset fields to the last saved values. |

Table 21 Field definition for Management>SNMP

# 6.4. Log

The “Management>Log” will display system log output as shown in Figure 31. The “Refresh” button will clear the log window and display the most current system log information.

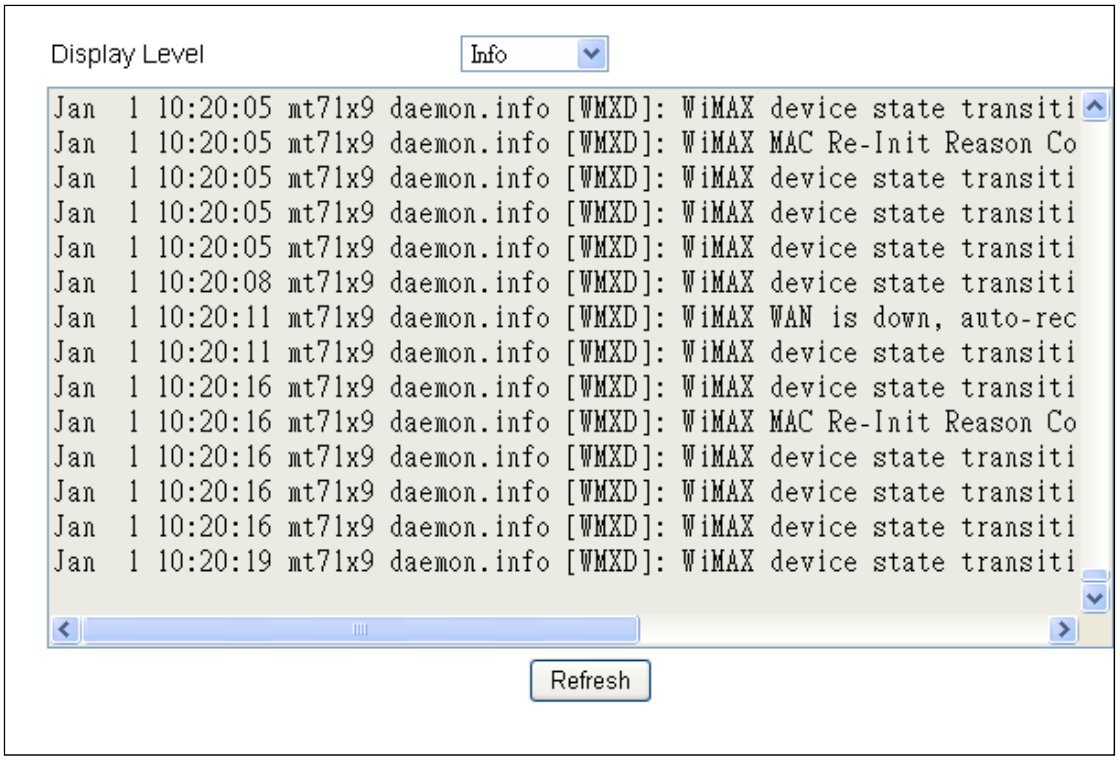
Display Level
Info
Jan 1 10:20:05 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:05 mt71x9 daemon.info [WMXD]: WiMAX MAC Re-Init Reason Co
Jan 1 10:20:05 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:05 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:05 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:08 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:11 mt71x9 daemon.info [WMXD]: WiMAX WAN is down, auto-rec
Jan 1 10:20:11 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:16 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:16 mt71x9 daemon.info [WMXD]: WiMAX MAC Re-Init Reason Co
Jan 1 10:20:16 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:16 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:16 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Jan 1 10:20:19 mt71x9 daemon.info [WMXD]: WiMAX device state transiti
Refresh

Figure 31 Management>Log

# 6.5. Upgrade

The “Upgrade” window allows user to upgrade the firmware on the device. Users can choose to upgrade the firmware by entering the file path as shown in Figure 32. The definition for each field is shown on Table 22.

Note: After pressing the “Upgrade” button. It will automatically reboot the CPE and upgrade the firmware with the specified file. User will be prompted to login to CPE after the upgrade is complete.

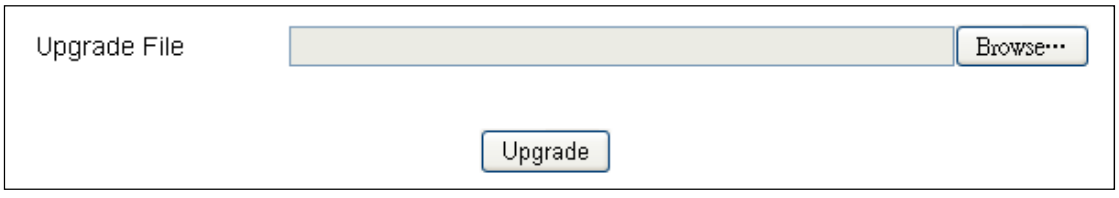


Figure 32 Management>Upgrade

| Name | Description |
|---|---|
| Browse | Enter the full path of the file user wants to upgrade. The "browse" button will help user to find the file on the server. |

| Name | Description |
|---|---|
| Upgrade | It will start upgrading the file |
| Status | The status bar will display which segment it's processing and what percentage of the upgrade has been completed. |

Table 22 Field definition for Management>Upgrade

# 6.6. Recovery

Recovery will set all the configurations back to factory defaults as shown in Figure 33. Any configurations that user has made will be changed back to the factory default settings. After selecting “Factory Default” button, it will prompt a window for user to confirm or cancel the action as shown in Figure 34.

Warning: Restore factory defaults will clear any IP addresses and setting that may have been configured on the CPE.

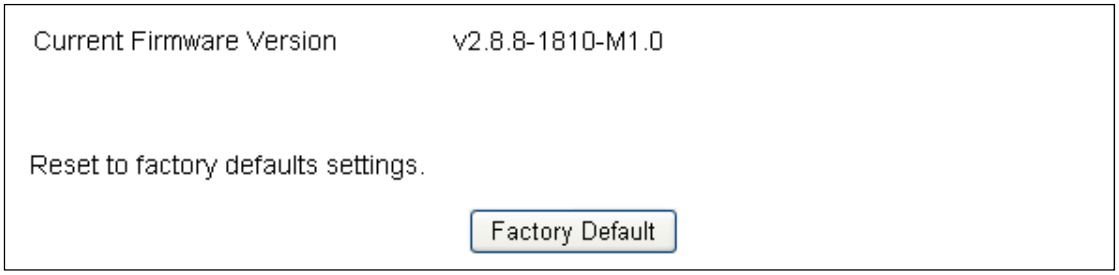


Figure 33 Management>Recovery

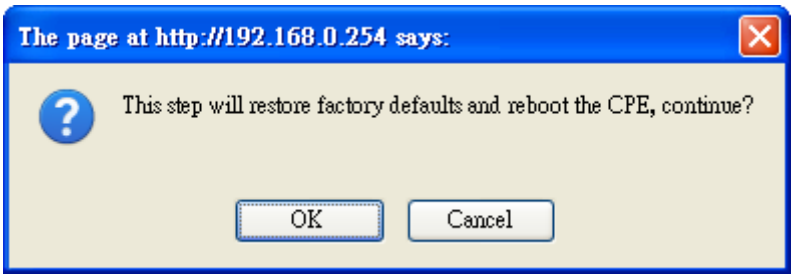


Figure 34 Restore to factory reset warning

# 7. VPN

VPN (Virtual Private Network) is a network that is implemented in an additional software layer on top of an existing larger network for the purpose of providing a secure extension of a private network into an insecure network such as the Internet. The links between nodes of a VPN are formed over logical connect-ions or virtual circuits between hosts of the larger network.

VPNs are often installed by organizations to provide remote access to a secure organizational network. Generally, a VPN has a network topology more compl- ex than a point-to-point connection. VPNs are also used to mask the IP address of individual computers within the Internet in order, for instance, to surf the World Wide Web anonymously or to access location restricted services, such as Internet television. Here, VPN Settings allow user to set rules for VPN, and it supports PPTP, L2TP, and IPsec.

## 7.1. PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP does not provide confidentiality or encryption; it relies on the protocol being tunneled to provide privacy.

### 7.1.1. PPTP Server

User can setup PPTP Server as shown in Figure 35. A PPTP Server (Point-To-Point Tunneling Protocol) allows user to connect securely from a place (such as the house) to a LAN located in another location, such as the office. This way user can use the services provided in the office at the comfort of the house. The definition for each field of PPTP Server is shown on Table 23.

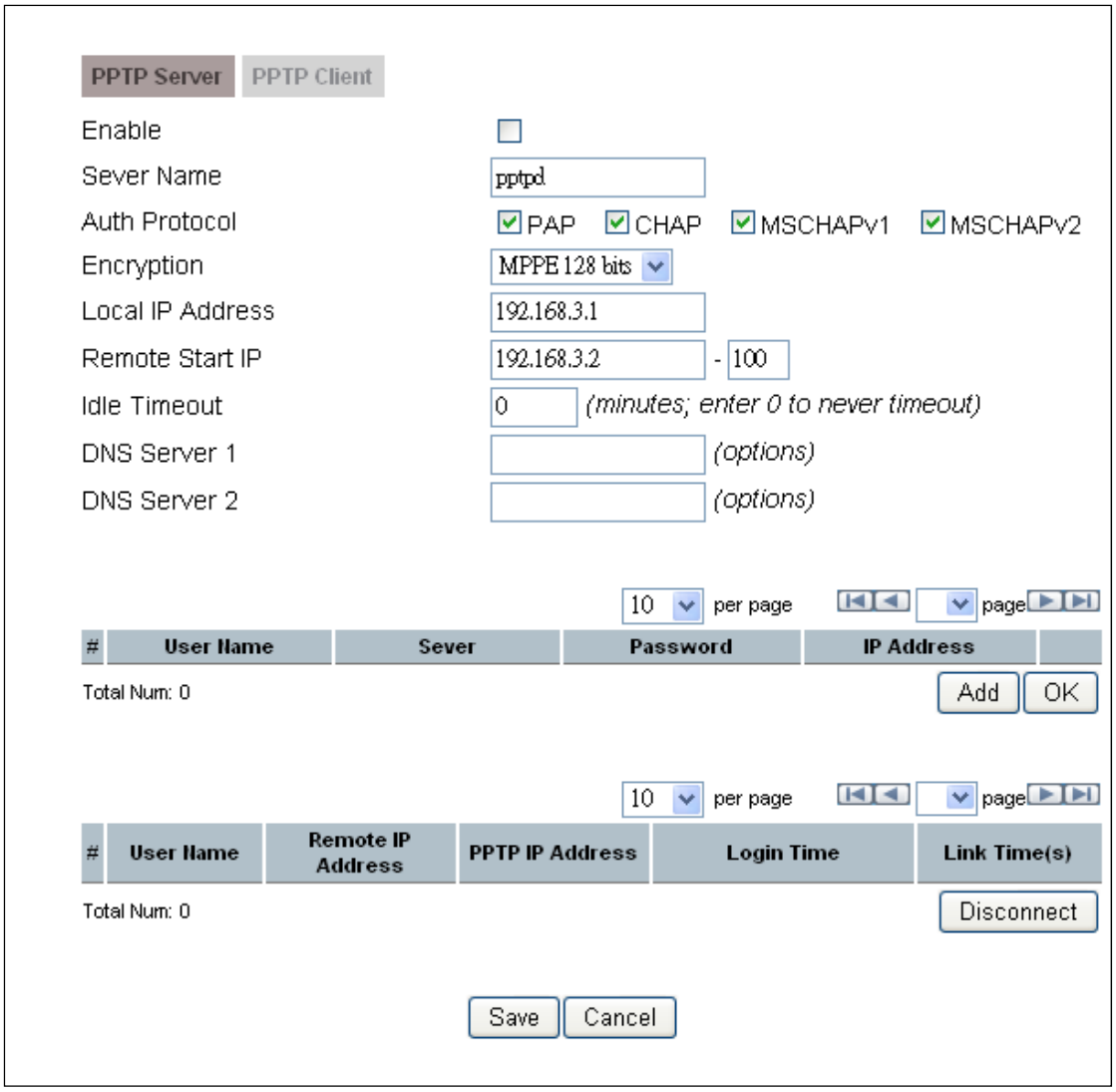


Figure 35 VPN>PPTP>PPTP Server

| Name | Description |
|---|---|
| **PPTP Server** | |
| Enable | Activate PPTP server. |
| Server Name | Offer a service name |
| Auth Protocol | Require the peer to authenticate itself before allowing network packets to be sent or received. We support the following protocol:<br>● PAP: Password Authentication Protocol<br>● CHAP: Challenge Handshake Authentication Protocol<br>● MSCHAP: Microsoft Challenge Handshake Authentication Protocol |

| Name | Description |
|---|---|
| | ● MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol, Version 2 |
| Encryption | Encryption Scheme:<br>● No<br>● MPPE 40 bits: 40-bit encryption with MPPE<br>● MPPE 128 bits: 128-bit encryption with MPPE<br>● Auto: automatically select |
| Local IP Address | The IP of router |
| Remote Start IP | As sessions are established, IP addresses are assigned starting from “Remote Start IP” |
| Idle Timeout | Disconnect if the link is idle for the assigned seconds |
| DNS Server 1 | The primary DNS (Domain Name Server) addresses to clients |
| DNS Server 2 | The secondary DNS (Domain Name Server) addresses to clients |
| **User Access List** | |
| User name | User ID to connect PPTP server via the selected Auth Protocol |
| Server | Server protocol type |
| Password | Password to connect PPTP server via the selected Auth Protocol |
| IP address | IP address of the connected client |
| **Connection List** | |
| User name | The user name of the connection |
| Remote IP address | The peer address of the connection |
| PPTP IP address | The assigned IP address of PPTP |
| Login Time | The time of the connection created |
| Link Time(s) | Timer from the connected time |
| Save | Commit the changes made and save to the CPE |
| Cancel | Reset fields to the last saved values |

Table 23 Field definition for VPN>PPTP>PPTP Server

## 7.1.2. PPTP Client

User could setup PPTP Client as shown in Figure 36 and Figure 37. The defi-

nition for each field of PPTP Client is shown on Table 24.

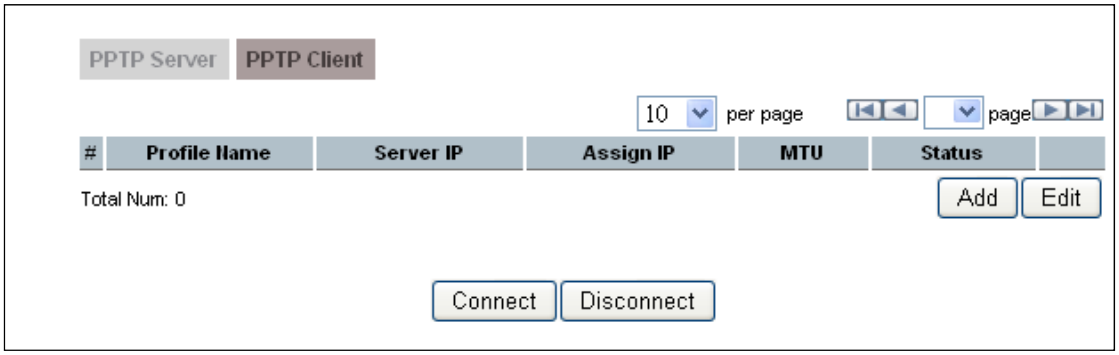


Figure 36 VPN>PPTP>PPTP Client

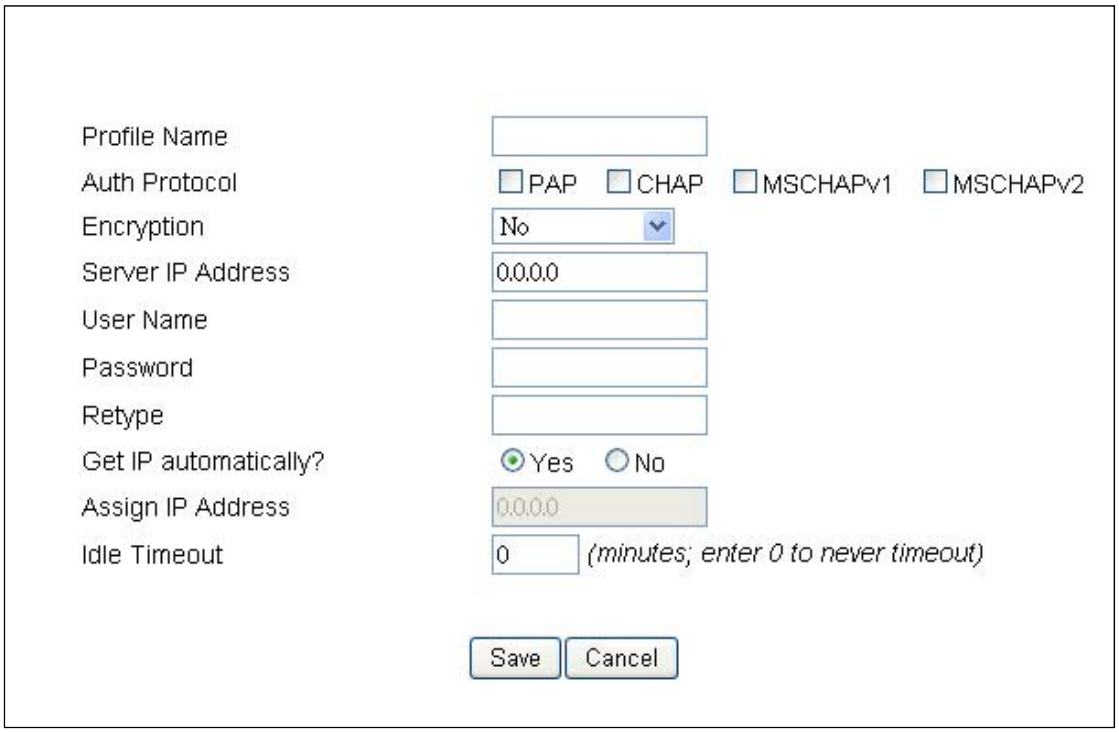


Figure 37 VPN>PPTP>PPTP Client>Add

| Name | Description |
|---|---|
| **PPTP Client** | |
| Add | Add a new connection setting |
| Edit | Edit the existed connection setting |
| **Edit PPTP Client** | |
| Profile Name | The name for this connection setting |
| Auth Protocol | The Authentication protocol of the peer required. Select which Authentication protocol to use.<br>● PAP |

| Name | Description |
|---|---|
| | ● CHAP<br>● MSCHAPv1<br>● MSCHAPv2 |
| Encryption | Encryption scheme |
| Server IP Address | The IP address of PPTP server |
| Username | The user ID to connect PPTP server via the selected Auth Protocol |
| Password | The password of the corresponding user ID |
| Retype | Type the “Password” again |
| Get IP automatically? | Obtain the dynamic IP address, assigned by the PPTP server |
| Assign IP Address | Assign the static IP address for this connection setting |
| Idle Timeout | Disconnect if the link is idle for the assigned seconds |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 24 Field definition for VPN>PPTP>PPTP Client

# 7.2. L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs). It does not provide any encryption or confidentiality by itself. It relies on an encryption protocol that it passes within the tunnel to provide privacy. The entire L2TP packet, including payload and L2TP header, is sent within a UDP datagram. It is common to carry Point-to-Point Protocol (PPP) session within an L2TP tunnel. L2TP does not provide confidentiality or strong authentication by itself. IPsec is often used to secure L2TP packets by providing confidentiality, authentication and integrity.

## 7.2.1. L2TP Server

User can setup CPE from web page as shown in Figure 38. The definition for each field of PPTP Server is shown on Table 25.

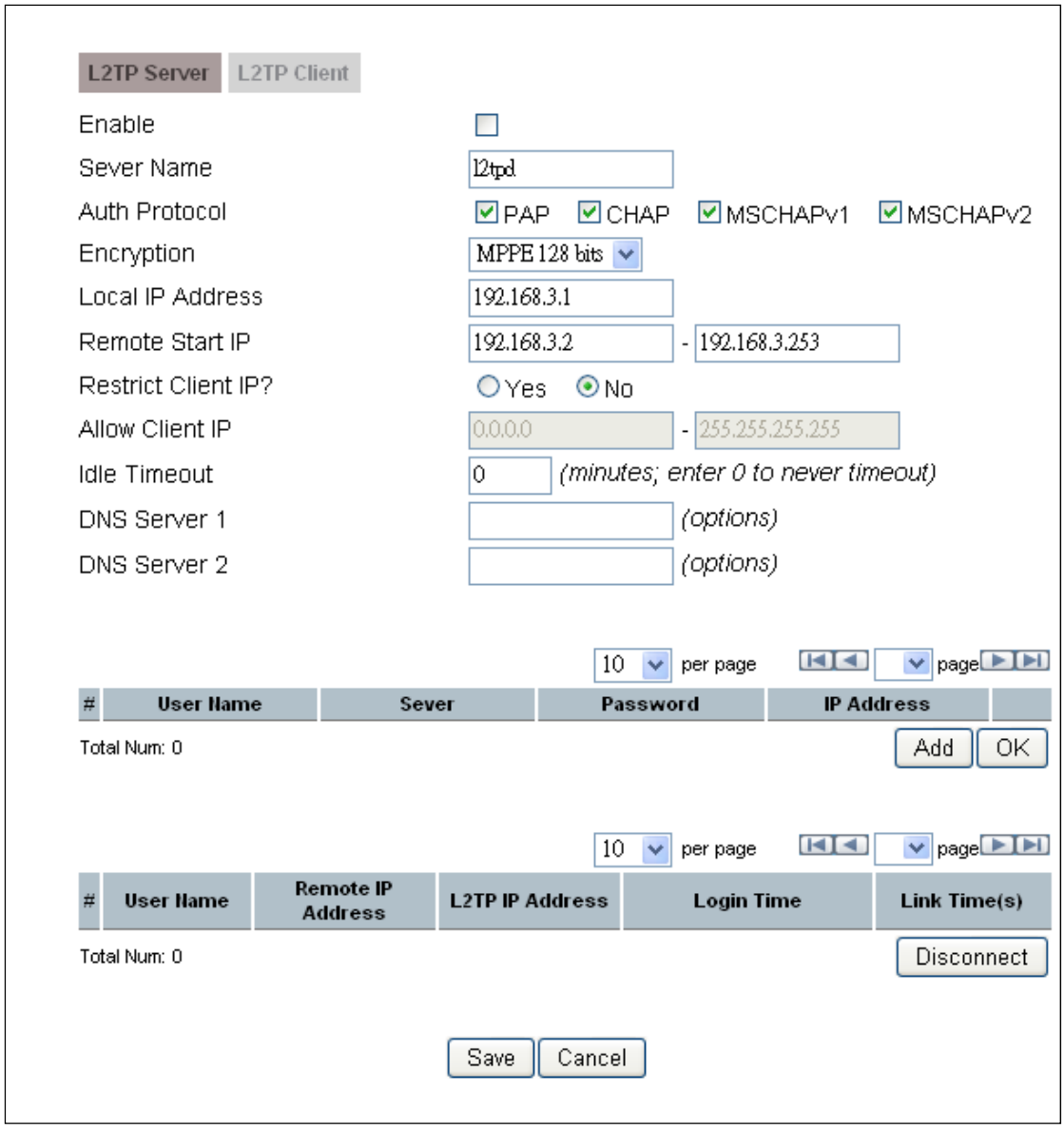


Figure 38 VPN>L2TP>L2TP Server

| Name | Description |
|---|---|
| **L2TP Server** | |
| Enable | Check the check box to activate L2TP server. |
| Server Name | Enter a service name |
| Auth Protocol | Require the peer to authenticate itself before allowing network packets to be sent or received. The following protocols are supported:<br>● PAP: Password Authentication Protocol<br>● CHAP: Challenge Handshake Authentication protocol<br>● MSCHAPv1: Microsoft Challenge Handshake |

| Name | Description |
|---|---|
| | Authentication Protocol<br>● MSCHAPv2: Microsoft Challenge Handshake Authentication Protocol, Version 2 |
| Encryption | Encryption Scheme<br>● No<br>● MPPE 40 bits: 40-bit encryption with MPPE<br>● MPPE 128 bits: 128-bit encryption with MPPE<br>● Auto: automatically select |
| Local IP Address | The IP of router |
| Remote Start IP | As sessions are established, IP addresses are assigned starting from “Remote Start IP” |
| Restrict Client IP? | To restrict client IP address range for the client |
| Allow Client IP | The IP address range for the client |
| Idle Timeout | Disconnect if the link is idle for the given number of seconds |
| DNS Server 1 | The primary DNS (Domain Name Server) addresses to the clients |
| DNS Server 2 | The secondary DNS (Domain Name Server) addresses to the clients |
| **User Access List** | |
| User Name | User ID to connect L2TP server via the selected Auth Protocol |
| Server | Server Protocol type |
| Password | Password to connect L2TP server via the selected Auth Protocol |
| IP Address | IP address of the connected client |
| **Connection List** | |
| User Name | The user name of the connection |
| Remote IP Address | The peer address of the connection |
| L2TP IP Address | The assigned IP address of L2TP |
| Login Time | The time of the connection created |
| Link Time(s) | Elapsed time connected |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 25 Field definition for VPN>L2TP>L2TP Server

## 7.2.2. L2TP Client

User could setup PPTP Client as shown in Figure 39 and Figure 40. The definition for each field of PPTP Client is shown on Table 26.

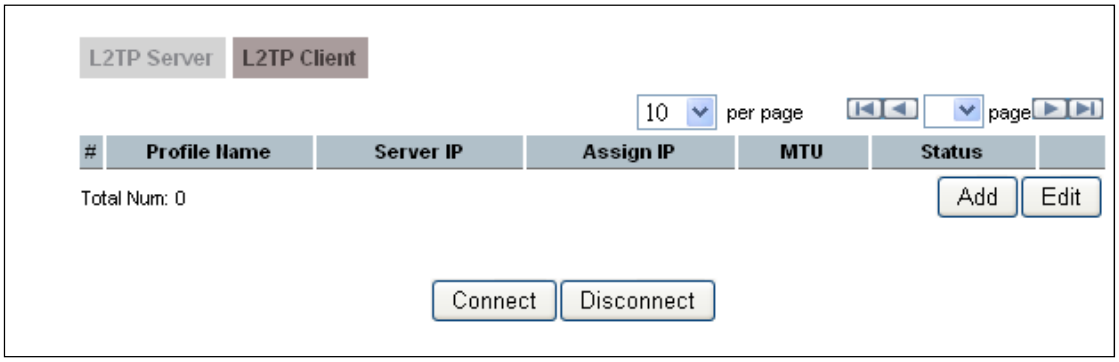


Figure 39 VPN>L2TP>L2TP Client

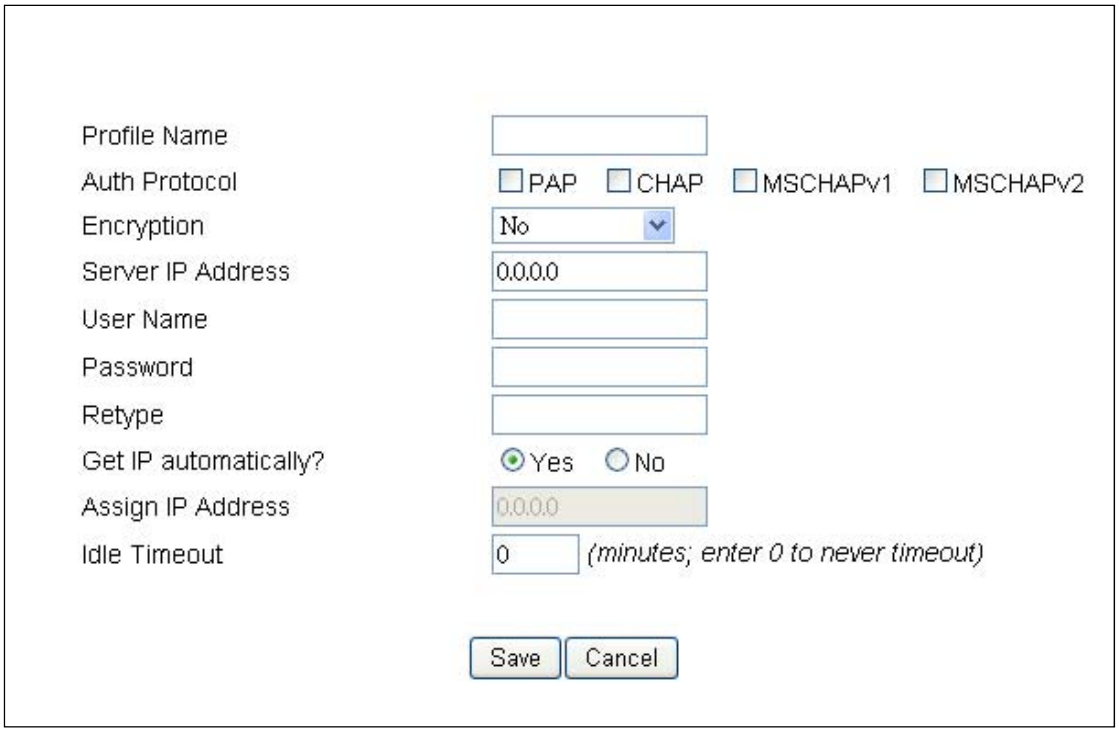


Figure 40 VPN>L2TP>L2TP Client>Add

| Name | Description |
|---|---|
| **L2TP Client** | |
| Add | Add a new connection setting |
| Edit | Edit the existed connection setting |
| **Edit L2TP Client** | |
| Profile Name | The name of this connection setting |

| Name | Description |
|---|---|
| Auth Protocol | The Authentication Protocol of the peer required. Select which Authentication protocol to use.<br>● PAP<br>● CHAP<br>● MSCHAPv1<br>● MSCHAPv2 |
| Encryption | Encryption Scheme |
| Server IP Address | The IP address of L2TP server |
| Username | The username to connect L2TP server via the selected Auth Protocol |
| Password | The password of the corresponding username |
| Retype | Type the “Password” again |
| Get IP Automatically? | Obtain the dynamic IP address, assigned by the L2TP server |
| Assign IP Address | Assign the static IP address for this connection setting |
| Idle Timeout | Disconnect if the link is idle for the assigned seconds |
| Save | Commit the changes made and save to CPE |
| Cancel | Reset fields to the last saved values |

Table 26 Field definition for VPN>L2TP>L2TP Client

# 7.3. IPsec

Internet Protocol Security (IPsec) is an end-to-end security solution and operated at the IP Layer. It provides secure communication between pairs of hosts, pairs of security gateways or between security gateways and a host. It’s based on a suite of protocols for securing IP traffic by authenticating and encrypting each IP packet of the data stream. User could setup IPsec as shown in Figure 41 and Figure 42. The definition for each field of PPTP Client is shown on Table 26.

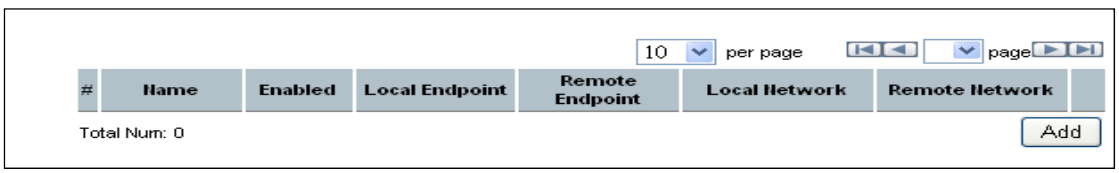


Figure 41 VPN>IPsec Overview

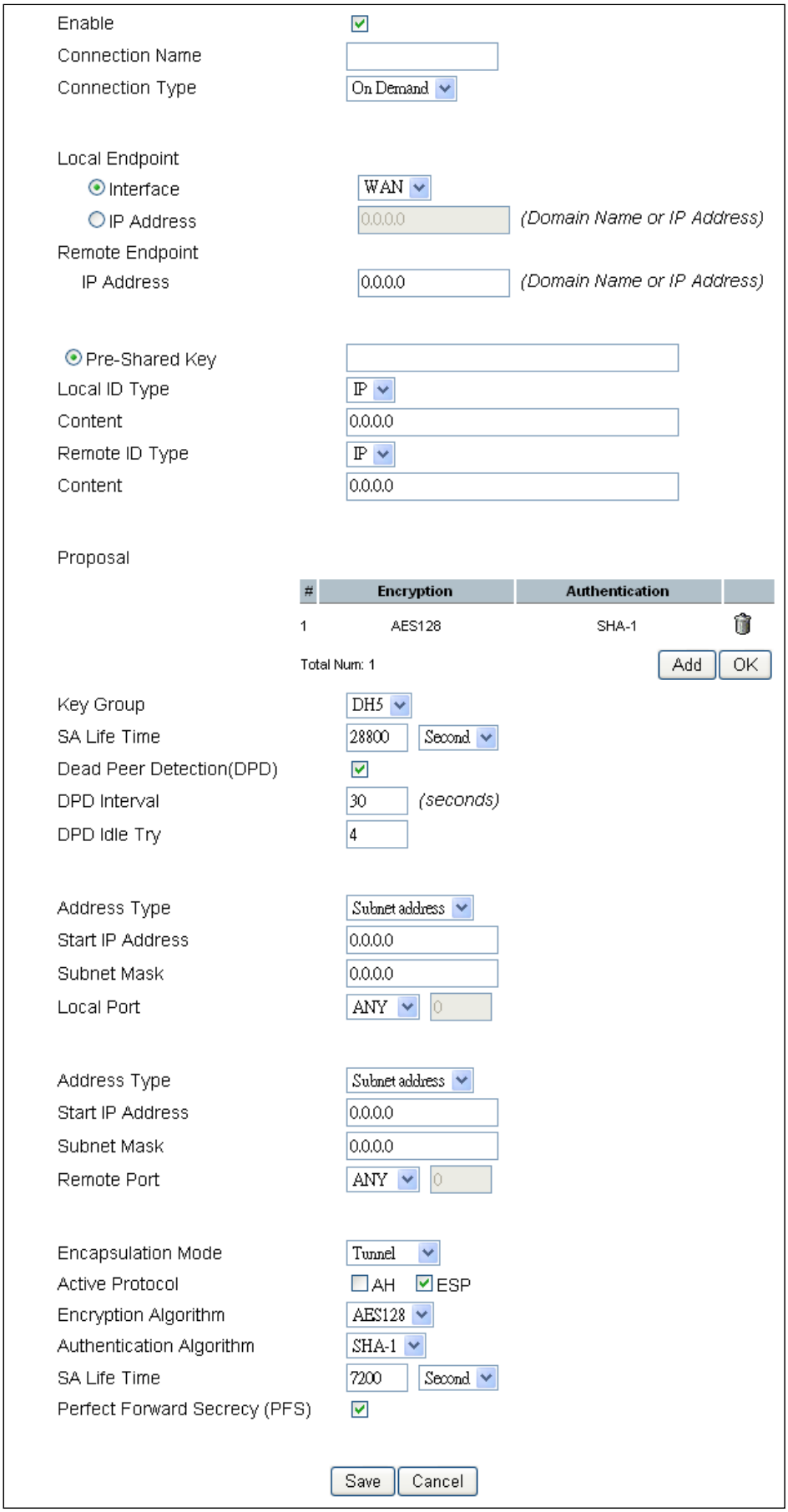


Figure 42 VPN>IPsec>Add

| Name | Description |
|---|---|
| Add | Click the "Add" button to add an IPsec connection rule |
| **Property** | |
| Enable | Enable IPsec connection. |
| Connection Name | The name of the connection |
| Connection Type | Select the connection type<br>● Initiator<br>● On Demand<br>● Responder |
| **Gateway Information** | |
| Local Endpoint Interface | The interface of the CPE public-network interface |
| Local Endpoint IP Address | The IP address or Domain Name of the CPE public-network interface |
| Remote Endpoint IP Address | The IP address or Domain Name of the remote peer. |
| **Authentication Method** | |
| Pre-Shared Key | The pre-share key that two security gateways use to authenticate |
| Local ID Type | States how the CPE should be identified for authentication<br><br>IP: The CPE is identified by the assigned IP for authentication. The default value is 0.0.0.0. |
| Content | The IP address |
| Remote ID Type | States how the remote peer should be identified for authentication<br><br>IP: The remote peer is identified by the assigned IP for authentication. The default value is 0.0.0.0, and this means CPE will accept any IP. |
| Content | The IP address |
| **IKE Phase 1** | |
| Proposal Add | Press the Add button to enter an Encryption and Authentication algorithm. Click the trash to remove the selected algorithm. Encryption Algorithm:<br>● DES<br>● 3DES |

| Name | Description |
|---|---|
| | ● AES128<br>● AES192<br>● AES256<br><br>Authentication Algorithm:<br>● MD5<br>● SHA-1 |
| Proposal OK | Click the OK button to exit the table edit mode |
| Key Group | The DH group used to negotiate the IKE/ISAKMP SA. |
| SA Life Time | The period that the keying channel of a connection (IKE/ISAKMP SA) should last before being rene-gotiated. |
| Dead Peer Detection (DPD) | Enable or disable the Dead Peer Detection protocol (RFC 3706) |
| DPD Interval | The time interval when R_U_THERE messages are sent to the peer. |
| DPD Idle Try | The retry counter for DPD. The timeout interval is "DPD interval" multiplied by "DPD Idle Try". After the timeout interval all connections to the peer are deleted if they are inactive. |
| **Local Network** | The private subnet behind the CPE. |
| Address Type | Single Address: The private subnet consisting of one IP address.<br><br>Subnet address: The private subnet consisting within the subnet IP addresses. |
| Start IP Address | The only IP address allowed in the subnet |
| Subnet Mask | The netmask of the subnet (Subnet address) |
| Local Port | Restrict the traffic selector to a single protocol and/or port.<br>● Any: No restriction<br>● ICMP: Restrict the traffic selector to ICMP protocol.<br>● TCP: Restrict the traffic selector to TCP protocol. If the port number is 0, all TCP port numbers are accepted.<br>● UDP: Restrict the traffic selector to UDP protocol. |

| Name | Description |
|---|---|
| | If the port number is 0, all UDP port numbers are accepted. |
| **Remote Network** | The private subnet behind the remote peer. |
| Address Type | Single Address: The private subnet consisting of one IP address.<br>Subnet address: The private subnet consisting of subnet IP addresses. |
| Start IP Address | The only IP address allowed in the subnet |
| Subnet Mask | The netmask of the subnet (Subnet address) |
| Remote Port | Restrict the traffic selector to a single protocol and/or port.<br>● Any: No restriction<br>● ICMP: Restrict the traffic selector to ICMP protocol.<br>● TCP: Restrict the traffic selector to TCP protocol. If the port number is 0, all TCP port numbers are accepted.<br>● UDP: Restrict the traffic selector to UDP protocol. If the port number is 0, all UDP port numbers are accepted. |
| **IPSec Proposal** | |
| Encapsulation Mode | The type of the connection:<br>● Tunnel: signifying a host-to-host, host-to-subnet, or subnet-to subnet tunnel.<br>● Transport: signifying host-to-host transport made. |
| Active Protocol | Whether authentication should be done as part of ESP encryption and/or separately using the AH protocol. |
| Encryption Algorithm | ● NULL<br>● AES128<br>● AES192<br>● AES256<br>● DES<br>● 3DES |
| Authentication Algorithm | ● MD5<br>● SHA-1 |
| SA Life Time | The time interval a particular instance of a connection |

| Name | Description |
|---|---|
| | (a set of encryption/authentication key for user packets) should last, from successful negotiation to expiry. |
| Perfect Forward Secrecy (PFS) | Whether Perfect Forward Secrecy of keys is desired on the connection's keying channel. |
| Save | Commit the changes made and save to the CPE device |
| Cancel | Reset fields to the last saved values. |

Table 27 Field definition for VPN>IPsec>Add